National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Jun 2020 Vol. 07 No. 11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
access-policy_project					
access-policy					
Improper Input Validation	10-06-2020	7.5	access-policy through 3.1.0 is vulnerable to Arbitrary Code Execution. User input provided to the `template` function is executed by the `eval` function resulting in code execution. **CVE ID : CVE-2020-7674**	N/A	A-ACC-ACCE-060820/1
Adobe					
experience_manager					
Server-Side Request Forgery (SSRF)	12-06-2020	5	Adobe Experience Manager versions 6.5 and earlier have a server-side request forgery (ssrf) vulnerability. Successful exploitation could lead to sensitive information disclosure. **CVE ID : CVE-2020-9643**	https://helpx.adobe.com/security/products/experience-manager/apsb20-31.html	A-ADO-EXPE-060820/2
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2020	3.5	Adobe Experience Manager versions 6.5 and earlier have a cross-site scripting (stored) vulnerability. Successful exploitation could lead to arbitrary javascript execution in the browser. **CVE ID : CVE-2020-9644**	https://helpx.adobe.com/security/products/experience-manager/apsb20-31.html	A-ADO-EXPE-060820/3
Server-Side Request Forgery (SSRF)	12-06-2020	5	Adobe Experience Manager versions 6.5 and earlier have a blind server-side request forgery (ssrf) vulnerability.	https://helpx.adobe.com/security/products/	A-ADO-EXPE-060820/4

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation could lead to sensitive information disclosure. **CVE ID : CVE-2020-9645**	experience-manager/apsb20-31.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2020	4.3	Adobe Experience Manager versions 6.5 and earlier have a cross-site scripting (dom-based) vulnerability. Successful exploitation could lead to arbitrary javascript execution in the browser. **CVE ID : CVE-2020-9647**	https://helpx.adobe.com/security/products/experience-manager/apsb20-31.html	A-ADO-EXPE-060820/5
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2020	4.3	Adobe Experience Manager versions 6.5 and earlier have a cross-site scripting vulnerability. Successful exploitation could lead to arbitrary javascript execution in the browser. **CVE ID : CVE-2020-9648**	https://helpx.adobe.com/security/products/experience-manager/apsb20-31.html	A-ADO-EXPE-060820/6
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2020	4.3	Adobe Experience Manager versions 6.5 and earlier have a cross-site scripting (reflected) vulnerability. Successful exploitation could lead to arbitrary javascript execution in the browser. **CVE ID : CVE-2020-9651**	https://helpx.adobe.com/security/products/experience-manager/apsb20-31.html	A-ADO-EXPE-060820/7
flash_player					
Use After Free	12-06-2020	10	Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free	https://helpx.adobe.com/security/products/flash-player/apsb20-30.html	A-ADO-FLAS-060820/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9633**		
flash_player_desktop_runtime					
Use After Free	12-06-2020	10	Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9633**	https://helpx.adobe.com/security/products/flash-player/apsb20-30.html	A-ADO-FLAS-060820/9
framemaker					
Out-of-bounds Write	12-06-2020	6.8	Adobe Framemaker versions 2019.0.5 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9634**	https://helpx.adobe.com/security/products/framemaker/apsb20-32.html	A-ADO-FRAM-060820/10
Out-of-bounds Write	12-06-2020	6.8	Adobe Framemaker versions 2019.0.5 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9635**	https://helpx.adobe.com/security/products/framemaker/apsb20-32.html	A-ADO-FRAM-060820/11
Improper Restriction of Operations within the	12-06-2020	6.8	Adobe Framemaker versions 2019.0.5 and below have a memory corruption vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/framemaker	A-ADO-FRAM-060820/12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			arbitrary code execution. **CVE ID : CVE-2020-9636**	/apsb20-32.html	
Advantech					
webaccess					
Out-of-bounds Write	15-06-2020	7.5	WebAccess Node Version 8.4.4 and prior is vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2020-12019**	N/A	A-ADV-WEBA-060820/13
angularjs					
angular.js					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-06-2020	3.5	angular.js prior to 1.8.0 allows cross site scripting. The regex-based input HTML replacement may turn sanitized code into unsanitized one. Wrapping "<option>" elements in "<select>" ones changes parsing behavior, leading to possibly unsanitizing code. **CVE ID : CVE-2020-7676**	N/A	A-ANG-ANGU-060820/14
anydesk					
anydesk					
Use of Externally-Controlled Format String	09-06-2020	7.5	AnyDesk before 5.5.3 on Linux and FreeBSD has a format string vulnerability that can be exploited for remote code execution. **CVE ID : CVE-2020-13160**	N/A	A-ANY-ANYD-060820/15
Apache					
ignite					
Incorrect	03-06-2020	6.4	Apache Ignite uses H2	N/A	A-APA-IGNI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			database to build SQL distributed execution engine. H2 provides SQL functions which could be used by attacker to access to a filesystem. **CVE ID : CVE-2020-1963**		060820/16
karaf					
Server-Side Request Forgery (SSRF)	12-06-2020	6.5	In Karaf, JMX authentication takes place using JAAS and authorization takes place using ACL files. By default, only an "admin" can actually invoke on an MBean. However there is a vulnerability there for someone who is not an admin, but has a "viewer" role. In the 'etc/jmx.acl.cfg', such as role can call get*. It's possible to authenticate as a viewer role + invokes on the MLet getMBeansFromURL method, which goes off to a remote server to fetch the desired MBean, which is then registered in Karaf. At this point the attack fails as "viewer" doesn't have the permission to invoke on the MBean. Still, it could act as a SSRF style attack and also it essentially allows a "viewer" role to pollute the MBean registry, which is a kind of privilege escalation. The vulnerability is low as it's possible to add a ACL to limit access. Users should update to Apache Karaf 4.2.9 or	N/A	A-APA-KARA-060820/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			newer. **CVE ID : CVE-2020-11980**		
tomee					
Improper Authenticati on	15-06-2020	6.8	If Apache TomEE is configured to use the embedded ActiveMQ broker, and the broker URI includes the useJMX=true parameter, a JMX port is opened on TCP port 1099, which does not include authentication. This affects Apache TomEE 8.0.0-M1 - 8.0.1, Apache TomEE 7.1.0 - 7.1.2, Apache TomEE 7.0.0-M1 - 7.0.7, Apache TomEE 1.0.0 - 1.7.5. **CVE ID : CVE-2020-11969**	N/A	A-APA-TOME-060820/18
unomi					
Improper Input Validation	05-06-2020	10	Apache Unomi allows conditions to use OGNL scripting which offers the possibility to call static Java classes from the JDK that could execute code with the permission level of the running Java process. **CVE ID : CVE-2020-11975**	N/A	A-APA-UNOM-060820/19
Apple					
watchos					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious	N/A	A-APP-WATC-060820/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9813**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9814**	N/A	A-APP-WATC-060820/21
windows_migration_assistant					
Uncontrolled Search Path Element	09-06-2020	4.4	A dynamic library loading issue was addressed with improved path searching. This issue is fixed in Windows Migration Assistant 2.2.0.0 (v. 1A11). Running the installer in an untrusted directory may result in arbitrary code execution. **CVE ID : CVE-2020-9858**	N/A	A-APP-WIND-060820/22
icloud					
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for	N/A	A-APP-ICLO-060820/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9789**		
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9790**	N/A	A-APP-ICLO-060820/24
Out-of-bounds Read	09-06-2020	5.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A malicious application may cause a denial of service or potentially disclose memory contents. **CVE ID : CVE-2020-9794**	N/A	A-APP-ICLO-060820/25
Access of Resource Using Incompatible Type ('Type	09-06-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5,	N/A	A-APP-ICLO-060820/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Confusion')			watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9800**		
N/A	09-06-2020	6.8	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9802**	N/A	A-APP-ICLO-060820/27
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9803**	N/A	A-APP-ICLO-060820/28
Improper Neutralizatio n of Input	09-06-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5	N/A	A-APP-ICLO-060820/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9805**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9806**	N/A	A-APP-ICLO-060820/30
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9807**	N/A	A-APP-ICLO-060820/31
Improper	09-06-2020	4.3	An input validation issue	N/A	A-APP-ICLO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9843**		060820/32
N/A	09-06-2020	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-9850**	N/A	A-APP-ICLO-060820/33
itunes					
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution.	N/A	A-APP-ITUN-060820/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9789		
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9790**	N/A	A-APP-ITUN-060820/35
Out-of-bounds Read	09-06-2020	5.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A malicious application may cause a denial of service or potentially disclose memory contents. **CVE ID : CVE-2020-9794**	N/A	A-APP-ITUN-060820/36
Access of Resource Using Incompatible Type ('Type Confusion')	09-06-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously	N/A	A-APP-ITUN-060820/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9800**		
N/A	09-06-2020	6.8	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9802**	N/A	A-APP-ITUN-060820/38
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9803**	N/A	A-APP-ITUN-060820/39
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19.	N/A	A-APP-ITUN-060820/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9805**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9806**	N/A	A-APP-ITUN-060820/41
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9807**	N/A	A-APP-ITUN-060820/42
Improper Neutralization of Input During Web Page Generation	09-06-2020	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1,	N/A	A-APP-ITUN-060820/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9843**		
N/A	09-06-2020	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-9850**	N/A	A-APP-ITUN-060820/44
safari					
Access of Resource Using Incompatible Type ('Type Confusion')	09-06-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9800**	N/A	A-APP-SAFA-060820/45
N/A	09-06-2020	4.6	A logic issue was addressed with improved restrictions. This issue is fixed in Safari 13.1.1. A malicious process	N/A	A-APP-SAFA-060820/46

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may cause Safari to launch an application. **CVE ID : CVE-2020-9801**		
N/A	09-06-2020	6.8	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9802**	N/A	A-APP-SAFA-060820/47
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9803**	N/A	A-APP-SAFA-060820/48
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously	N/A	A-APP-SAFA-060820/49

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9805**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9806**	N/A	A-APP-SAFA-060820/50
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9807**	N/A	A-APP-SAFA-060820/51
Improper Neutralization of Input During Web Page Generation ('Cross-site	09-06-2020	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows,	N/A	A-APP-SAFA-060820/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9843**		
N/A	09-06-2020	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-9850**	N/A	A-APP-SAFA-060820/53
Arista					
cloudeos					
N/A	10-06-2020	4.3	A vulnerability exists in Arista's Cloud EOS VM / vEOS 4.23.2M and below releases in the 4.23.x train, 4.22.4M and below releases in the 4.22.x train, 4.21.3M to 4.21.9M releases in the 4.21.x train, 4.21.3FX-7368.*, 4.21.4-FCRFX.*, 4.21.4.1, 4.21.7.1, 4.22.2.0.1, 4.22.2.2.1, 4.22.3.1, and 4.23.2.1 Router code in a scenario where TCP MSS options are configured. **CVE ID : CVE-2020-11622**	https://www.arista.com/en/support/advisories-notices/security-advisories/11195-security-advisory-49	A-ARI-CLOU-060820/54
veos					
N/A	10-06-2020	4.3	A vulnerability exists in	https://ww	A-ARI-VEOS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Arista's Cloud EOS VM / vEOS 4.23.2M and below releases in the 4.23.x train, 4.22.4M and below releases in the 4.22.x train, 4.21.3M to 4.21.9M releases in the 4.21.x train, 4.21.3FX-7368.*, 4.21.4-FCRFX.*, 4.21.4.1, 4.21.7.1, 4.22.2.0.1, 4.22.2.2.1, 4.22.3.1, and 4.23.2.1 Router code in a scenario where TCP MSS options are configured. **CVE ID : CVE-2020-11622**	w.arista.com/en/support/advisories-notices/security-advisories/11195-security-advisory-49	060820/55
Arubanetworks					
clearpass_policy_manager					
Missing Authentication for Critical Function	03-06-2020	10	The ClearPass Policy Manager web interface is affected by a vulnerability that leads to authentication bypass. Upon successful bypass an attacker could then execute an exploit that would allow to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher. **CVE ID : CVE-2020-7115**	N/A	A-ARU-CLEA-060820/56
Improper Input Validation	03-06-2020	9	The ClearPass Policy Manager WebUI administrative interface has an authenticated command remote execution. When the attacker is already authenticated to the administrative interface, they could then exploit the	N/A	A-ARU-CLEA-060820/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system, leading to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher. **CVE ID : CVE-2020-7116**		
N/A	03-06-2020	9	The ClearPass Policy Manager WebUI administrative interface has an authenticated command remote execution. When the attacker is already authenticated to the administrative interface, they could then exploit the system, leading to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher. **CVE ID : CVE-2020-7117**	N/A	A-ARU-CLEA-060820/58
Atlassian					
jira					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-06-2020	3.5	Affected versions are: Before 8.5.5, and from 8.6.0 before 8.8.1 of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the XML export view. **CVE ID : CVE-2020-4021**	N/A	A-ATL-JIRA-060820/59
companion					
Untrusted Search Path	01-06-2020	4.4	The file editing functionality in the Atlassian Companion	N/A	A-ATL-COMP-060820/60

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			App before version 1.0.0 allows local attackers to have the app run a different executable in place of the app's cmd.exe via a untrusted search path vulnerability. **CVE ID : CVE-2020-4019**		
N/A	01-06-2020	6.5	The file downloading functionality in the Atlassian Companion App before version 1.0.0 allows remote attackers, who control a Confluence Server instance that the Companion App is connected to, execute arbitrary .exe files via a Protection Mechanism Failure. **CVE ID : CVE-2020-4020**	N/A	A-ATL-COMP-060820/61
navigator_links					
Incorrect Authorization	03-06-2020	4	The CustomAppsRestResource list resource in Atlassian Navigator Links before version 3.3.23, from version 4.0.0 before version 4.3.7, from version 5.0.0 before 5.0.1, and from version 5.1.0 before 5.1.1 allows remote attackers to enumerate all linked applications, including those that are restricted or otherwise hidden, through an incorrect authorization check. **CVE ID : CVE-2020-4026**	N/A	A-ATL-NAVI-060820/62
jira_software_data_center					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-06-2020	3.5	Affected versions are: Before 8.5.5, and from 8.6.0 before 8.8.1 of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the XML export view. **CVE ID : CVE-2020-4021**	N/A	A-ATL-JIRA-060820/63
crucible					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-06-2020	3.5	The review resource in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to inject arbitrary HTML or Javascript via a cross site scripting (XSS) vulnerability through the review objectives. **CVE ID : CVE-2020-4013**	N/A	A-ATL-CRUC-060820/64
Incorrect Authorization	01-06-2020	4	The /profile/deleteWatch.do resource in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to remove another user's watching settings for a repository via an improper authorization vulnerability. **CVE ID : CVE-2020-4014**	N/A	A-ATL-CRUC-060820/65
Information Exposure	01-06-2020	4	The /json/fe/activeUserFinder.do resource in Altassian Fisheye and Crucible before version 4.8.1 allows remote attackers to view user user email addresses via a information disclosure vulnerability.	N/A	A-ATL-CRUC-060820/66

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4015		
Information Exposure	01-06-2020	5	The /plugins/servlet/jira-blockers/ resource in the crucible-jira-ril plugin in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to get the ID of configured Jira application links via an information disclosure vulnerability. **CVE ID : CVE-2020-4016**	N/A	A-ATL-CRUC-060820/67
Information Exposure	01-06-2020	5	The /rest/jira-ril/1.0/jira-rest/applinks resource in the crucible-jira-ril plugin in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to get information about any configured Jira application links via an information disclosure vulnerability. **CVE ID : CVE-2020-4017**	N/A	A-ATL-CRUC-060820/68
Cross-Site Request Forgery (CSRF)	01-06-2020	6.8	The setup resources in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to complete the setup process via a cross-site request forgery (CSRF) vulnerability. **CVE ID : CVE-2020-4018**	N/A	A-ATL-CRUC-060820/69
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-06-2020	4.3	The review coverage resource in Atlassian Fisheye and Crucible before version 4.8.2 allows remote attackers to inject arbitrary HTML or Javascript via a cross site scripting (XSS) vulnerability through the	N/A	A-ATL-CRUC-060820/70

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			committerFilter parameter. **CVE ID : CVE-2020-4023**		
fisheye					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-06-2020	3.5	The review resource in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to inject arbitrary HTML or Javascript via a cross site scripting (XSS) vulnerability through the review objectives. **CVE ID : CVE-2020-4013**	N/A	A-ATL-FISH-060820/71
Incorrect Authorization	01-06-2020	4	The /profile/deleteWatch.do resource in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to remove another user's watching settings for a repository via an improper authorization vulnerability. **CVE ID : CVE-2020-4014**	N/A	A-ATL-FISH-060820/72
Information Exposure	01-06-2020	4	The /json/fe/activeUserFinder.do resource in Altassian Fisheye and Crucible before version 4.8.1 allows remote attackers to view user user email addresses via a information disclosure vulnerability. **CVE ID : CVE-2020-4015**	N/A	A-ATL-FISH-060820/73
Information Exposure	01-06-2020	5	The /plugins/servlet/jira-blockers/ resource in the crucible-jira-ril plugin in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to	N/A	A-ATL-FISH-060820/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			get the ID of configured Jira application links via an information disclosure vulnerability. **CVE ID : CVE-2020-4016**		
Information Exposure	01-06-2020	5	The /rest/jira-ril/1.0/jira-rest/applinks resource in the crucible-jira-ril plugin in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to get information about any configured Jira application links via an information disclosure vulnerability. **CVE ID : CVE-2020-4017**	N/A	A-ATL-FISH-060820/75
Cross-Site Request Forgery (CSRF)	01-06-2020	6.8	The setup resources in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to complete the setup process via a cross-site request forgery (CSRF) vulnerability. **CVE ID : CVE-2020-4018**	N/A	A-ATL-FISH-060820/76
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-06-2020	4.3	The review coverage resource in Atlassian Fisheye and Crucible before version 4.8.2 allows remote attackers to inject arbitrary HTML or Javascript via a cross site scripting (XSS) vulnerability through the committerFilter parameter. **CVE ID : CVE-2020-4023**	N/A	A-ATL-FISH-060820/77
Avaya					
ip_office					
Information Exposure	04-06-2020	2.1	A sensitive information disclosure vulnerability was	https://downloads.av	A-AVA-IP_O-060820/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			discovered in the web interface component of IP Office that may potentially allow a local user to gain unauthorized access to the component. Affected versions of IP Office include: 9.x, 10.0 through 10.1.0.7 and 11.0 though 11.0.4.3. **CVE ID : CVE-2020-7030**	aya.com/css/P8/documents/101067493	
Barton					
ngircd					
Out-of-bounds Read	15-06-2020	5	The Server-Server protocol implementation in ngIRCd before 26~rc2 allows an out-of-bounds access, as demonstrated by the IRC_NJOIN() function. **CVE ID : CVE-2020-14148**	N/A	A-BAR-NGIR-060820/79
beyondco					
ignition					
N/A	07-06-2020	7.5	The Ignition page before 2.0.5 for Laravel mishandles globals, _get, _post, _cookie, and _env. **CVE ID : CVE-2020-13909**	N/A	A-BEY-IGNI-060820/80
Bitdefender					
antivirus_2020					
Improper Link Resolution Before File Access ('Link Following')	05-06-2020	3.6	A vulnerability in the improper handling of symbolic links in Bitdefender Antivirus Free can allow an unprivileged user to substitute a quarantined file, and restore it to a privileged location. This issue affects	https://www.bitdefender.com/support/security-advisories/link-resolution-privilege-	A-BIT-ANTI-060820/81

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bitdefender Antivirus Free versions prior to 1.0.17.178. **CVE ID : CVE-2020-8103**	escalation-vulnerability-bitdefender-antivirus-free-va-8604/	
Bitrix					
bitrix24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-06-2020	4.3	modules/security/classes/general.post_filter.php/post_filter.php in the Web Application Firewall in Bitrix24 through 20.0.950 allows XSS by placing %00 before the payload. **CVE ID : CVE-2020-13758**	N/A	A-BIT-BITR-060820/82
bludit					
bludit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-06-2020	3.5	showAlert() in the administration panel in Bludit 3.12.0 allows XSS. **CVE ID : CVE-2020-13889**	N/A	A-BLU-BLUD-060820/83
Bolt					
bolt					
Cross-Site Request Forgery (CSRF)	08-06-2020	4.3	Bolt CMS before version 3.7.1 lacked CSRF protection in the preview generating endpoint. Previews are intended to be generated by the admins, developers, chief-editors, and editors, who are authorized to create content in the application.	https://github.com/bolt/bolt/security/advisories/GHSA-2q66-6cc3-6xm8	A-BOL-BOLT-060820/84

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			But due to lack of proper CSRF protection, unauthorized users could generate a preview. This has been fixed in Bolt 3.7.1 **CVE ID : CVE-2020-4040**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-06-2020	4.3	In Bolt CMS before version 3.7.1, the filename of uploaded files was vulnerable to stored XSS. It is not possible to inject javascript code in the file name when creating/uploading the file. But, once created/uploaded, it can be renamed to inject the payload in it. Additionally, the measures to prevent renaming the file to disallowed filename extensions could be circumvented. This is fixed in Bolt 3.7.1. **CVE ID : CVE-2020-4041**	https://github.com/bolt/bolt/security/advisories/GHSA-68q3-7wjp-7q3j	A-BOL-BOLT-060820/85
cd-messenger_project					
cd-messenger					
Improper Input Validation	10-06-2020	7.5	cd-messenger through 2.7.26 is vulnerable to Arbitrary Code Execution. User input provided to the `color` argument executed by the `eval` function resulting in code execution. **CVE ID : CVE-2020-7675**	N/A	A-CD--CD-M-060820/86
celluloid					
reel					
Inconsistent Interpretatio	01-06-2020	5	reel through 0.6.1 allows Request Smuggling attacks	N/A	A-CEL-REEL-060820/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of HTTP Requests ('HTTP Request Smuggling')			due to incorrect Content-Length and Transfer encoding header parsing. It is possible to conduct HTTP request smuggling attacks by sending the Content-Length header twice. Furthermore, invalid Transfer Encoding headers were found to be parsed as valid which could be leveraged for TE:CL smuggling attacks. Note: This project is deprecated, and is not maintained any more. **CVE ID : CVE-2020-7659**		
ciphermail					
gateway					
Improper Privilege Management	11-06-2020	9	An issue was discovered in CipherMail Community Gateway and Professional/Enterprise Gateway 1.0.1 through 4.7.1-0 and CipherMail Webmail Messenger 1.1.1 through 3.1.1-0. Attackers with administrative access to the web interface have multiple options to escalate their privileges to the Unix root account. **CVE ID : CVE-2020-12713**	N/A	A-CIP-GATE-060820/88
Inadequate Encryption Strength	11-06-2020	4.3	An issue was discovered in CipherMail Community Gateway Virtual Appliances and Professional/Enterprise Gateway Virtual Appliances versions 1.0.1 through 4.7.1-0 and CipherMail Webmail	N/A	A-CIP-GATE-060820/89

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Messenger Virtual Appliances 1.1.1 through 3.1.1-0. A Diffie-Hellman parameter of insufficient size could allow man-in-the-middle compromise of communications between CipherMail products and external SMTP clients. **CVE ID : CVE-2020-12714**		
webmail_messenger					
Improper Privilege Management	11-06-2020	9	An issue was discovered in CipherMail Community Gateway and Professional/Enterprise Gateway 1.0.1 through 4.7.1-0 and CipherMail Webmail Messenger 1.1.1 through 3.1.1-0. Attackers with administrative access to the web interface have multiple options to escalate their privileges to the Unix root account. **CVE ID : CVE-2020-12713**	N/A	A-CIP-WEBM-060820/90
Inadequate Encryption Strength	11-06-2020	4.3	An issue was discovered in CipherMail Community Gateway Virtual Appliances and Professional/Enterprise Gateway Virtual Appliances versions 1.0.1 through 4.7.1-0 and CipherMail Webmail Messenger Virtual Appliances 1.1.1 through 3.1.1-0. A Diffie-Hellman parameter of insufficient size could allow man-in-the-middle compromise of communications between CipherMail products and	N/A	A-CIP-WEBM-060820/91

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			external SMTP clients. **CVE ID : CVE-2020-12714**		
Cisco					
unified_contact_center_express					
Files or Directories Accessible to External Parties	03-06-2020	5.5	A vulnerability in the API subsystem of Cisco Unified Contact Center Express (Unified CCX) could allow an authenticated, remote attacker to change the availability state of any agent. The vulnerability is due to insufficient authorization enforcement on an affected system. An attacker could exploit this vulnerability by authenticating to an affected system with valid agent credentials and performing a specific API call with crafted input. A successful exploit could allow the attacker to change the availability state of an agent, potentially causing a denial of service condition. **CVE ID : CVE-2020-3267**	N/A	A-CIS-UNIF-060820/92
digital_network_architecture_center					
Information Exposure Through Log Files	03-06-2020	4	A vulnerability in the audit logging component of Cisco Digital Network Architecture (DNA) Center could allow an authenticated, remote attacker to view sensitive information in clear text. The vulnerability is due to the storage of certain unencrypted credentials. An	N/A	A-CIS-DIGI-060820/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by accessing the audit logs and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage network devices. **CVE ID : CVE-2020-3281**		
unified_computing_system					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	A-CIS-UNIF-060820/94
prime_infrastructure					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-06-2020	6.4	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability is due to improper validation of user-	N/A	A-CIS-PRIM-060820/95

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is stored in the underlying database. **CVE ID : CVE-2020-3339**		
webex_network_recording_player					
Improper Input Validation	03-06-2020	4.3	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful	N/A	A-CIS-WEBE-060820/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file. This vulnerability affects Cisco Webex Network Recording Player and Webex Player releases earlier than Release 3.0 MR3 Security Patch 2 and 4.0 MR3. **CVE ID : CVE-2020-3319**		
Improper Input Validation	03-06-2020	4.3	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash	N/A	A-CIS-WEBE-060820/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when trying to view the malicious file. **CVE ID : CVE-2020-3321**		
Improper Input Validation	03-06-2020	4.3	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file. **CVE ID : CVE-2020-3322**	N/A	A-CIS-WEBE-060820/98
identity_services_engine					
Concurrent Execution using Shared Resource	03-06-2020	4.3	A vulnerability in the syslog processing engine of Cisco Identity Services Engine (ISE) could allow an	N/A	A-CIS-IDEN-060820/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a race condition that may occur when syslog messages are processed. An attacker could exploit this vulnerability by sending a high rate of syslog messages to an affected device. A successful exploit could allow the attacker to cause the Application Server process to crash, resulting in a DoS condition. **CVE ID : CVE-2020-3353**		
application_policy_infrastructure_controller					
Missing Authentication for Critical Function	03-06-2020	5	A vulnerability in the API of Cisco Application Services Engine Software could allow an unauthenticated, remote attacker to update event policies on an affected device. The vulnerability is due to insufficient authentication of users who modify policies on an affected device. An attacker could exploit this vulnerability by crafting a malicious HTTP request to contact an affected device. A successful exploit could allow the attacker to update event policies on the affected device. **CVE ID : CVE-2020-3333**	N/A	A-CIS-APPL-060820/100
Missing Authenticati	03-06-2020	2.1	A vulnerability in the key store of Cisco Application	N/A	A-CIS-APPL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on for Critical Function			Services Engine Software could allow an authenticated, local attacker to read sensitive information of other users on an affected device. The vulnerability is due to insufficient authorization limitations. An attacker could exploit this vulnerability by logging in to an affected device locally with valid credentials. A successful exploit could allow the attacker to read the sensitive information of other users on the affected device. **CVE ID : CVE-2020-3335**		060820/101
nx-os					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a	N/A	A-CIS-NX-O-060820/102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
Improper Input Validation	03-06-2020	7.8	A vulnerability in Security Group Tag Exchange Protocol (SXP) in Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because crafted SXP packets are mishandled. An attacker could exploit this vulnerability by sending specifically crafted SXP packets to the affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3228**	N/A	A-CIS-NX-O-060820/103
iox					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	3.5	A vulnerability in the web-based Local Manager interface of the Cisco IOx Application Framework could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based Local Manager interface of an affected device. The attacker must have valid Local Manager credentials. The vulnerability is due to insufficient validation of user-supplied input by the web-based Local Manager interface of the affected software. An attacker could exploit this vulnerability by injecting malicious code into a system settings tab. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected web interface or allow the attacker to access sensitive browser-based information. **CVE ID : CVE-2020-3233**	N/A	A-CIS-IOX-060820/104
Improper Link Resolution Before File Access ('Link Following')	03-06-2020	4.6	A vulnerability in the Cisco Application Framework component of the Cisco IOx application environment could allow an authenticated, local attacker to overwrite arbitrary files in the virtual instance that is running on the affected device. The vulnerability is	N/A	A-CIS-IOX-060820/105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient path restriction enforcement. An attacker could exploit this vulnerability by including a crafted file in an application package. An exploit could allow the attacker to overwrite files. **CVE ID : CVE-2020-3237**		
Improper Input Validation	03-06-2020	5.5	A vulnerability in the Cisco Application Framework component of the Cisco IOx application environment could allow an authenticated, remote attacker to write or modify arbitrary files in the virtual instance that is running on the affected device. The vulnerability is due to insufficient input validation of user-supplied application packages. An attacker who can upload a malicious package within Cisco IOx could exploit the vulnerability to modify arbitrary files. The impacts of a successful exploit are limited to the scope of the virtual instance and do not affect the device that is hosting Cisco IOx. **CVE ID : CVE-2020-3238**	N/A	A-CIS-IOX-060820/106
webex_player					
Improper Input Validation	03-06-2020	4.3	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an	N/A	A-CIS-WEBE-060820/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file. This vulnerability affects Cisco Webex Network Recording Player and Webex Player releases earlier than Release 3.0 MR3 Security Patch 2 and 4.0 MR3. **CVE ID : CVE-2020-3319**		
Improper Input Validation	03-06-2020	4.3	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for	N/A	A-CIS-WEBE-060820/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file. **CVE ID : CVE-2020-3321**		
Improper Input Validation	03-06-2020	4.3	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording	N/A	A-CIS-WEBE-060820/109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file. **CVE ID : CVE-2020-3322**		
application_services_engine					
Missing Authenticati on for Critical Function	03-06-2020	5	A vulnerability in the API of Cisco Application Services Engine Software could allow an unauthenticated, remote attacker to update event policies on an affected device. The vulnerability is due to insufficient authentication of users who modify policies on an affected device. An attacker could exploit this vulnerability by crafting a malicious HTTP request to contact an affected device. A successful exploit could allow the attacker to update event policies on the affected device. **CVE ID : CVE-2020-3333**	N/A	A-CIS-APPL-060820/110
Missing Authenticati on for Critical	03-06-2020	2.1	A vulnerability in the key store of Cisco Application Services Engine Software could allow an	N/A	A-CIS-APPL-060820/111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			authenticated, local attacker to read sensitive information of other users on an affected device. The vulnerability is due to insufficient authorization limitations. An attacker could exploit this vulnerability by logging in to an affected device locally with valid credentials. A successful exploit could allow the attacker to read the sensitive information of other users on the affected device. **CVE ID : CVE-2020-3335**		
ucs_manager					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	A-CIS-UCS_-060820/112
Citrix					
workspace_app					
Incorrect Default Permissions	08-06-2020	7.2	Citrix Workspace App before 1912 on Windows has Insecure Permissions and an Unquoted Path vulnerability	https://support.citrix.com/article/CTX275460	A-CIT-WORK-060820/113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which allows local users to gain privileges during the uninstallation of the application. **CVE ID : CVE-2020-13884**		
Incorrect Default Permissions	08-06-2020	7.2	Citrix Workspace App before 1912 on Windows has Insecure Permissions which allows local users to gain privileges during the uninstallation of the application. **CVE ID : CVE-2020-13885**	https://support.citrix.com/article/CTX275460	A-CIT-WORK-060820/114
xenapp					
Information Exposure	11-06-2020	4.3	** UNSUPPORTED WHEN ASSIGNED ** Citrix XenApp 6.5, when 2FA is enabled, allows a remote unauthenticated attacker to ascertain whether a user exists on the server, because the 2FA error page only occurs after a valid username is entered. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2020-13998**	N/A	A-CIT-XENA-060820/115
cncf					
cni_network_plugins					
N/A	03-06-2020	6	A vulnerability was found in all versions of containernetworking/plugins before version 0.8.6, that allows malicious containers in Kubernetes clusters to perform man-in-the-middle	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10749	A-CNC-CNI_-060820/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(MitM) attacks. A malicious container can exploit this flaw by sending rogue IPv6 router advertisements to the host or other containers, to redirect traffic to the malicious container. **CVE ID : CVE-2020-10749**		
codedropz					
drag_and_drop_multiple_file_upload_-_contact_form_7					
Unrestricted Upload of File with Dangerous Type	08-06-2020	7.5	The drag-and-drop-multiple-file-upload-contact-form-7 plugin before 1.3.3.3 for WordPress allows Unrestricted File Upload and remote code execution by setting supported_type to php% and uploading a .php% file. **CVE ID : CVE-2020-12800**	https://wordpress.org/plugins/drag-and-drop-multiple-file-upload-contact-form-7/#developers	A-COD-DRAG-060820/117
Combodo					
itop					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-06-2020	4.3	In Combodo iTop a menu shortcut name can be exploited with a stored XSS payload. This is fixed in all iTop packages (community, essential, professional) in version 2.7.0 and iTop essential and iTop professional in version 2.6.4. **CVE ID : CVE-2020-11696**	https://github.com/Combodo/iTop/security/advisories/GHSA-4h6p-jghj-8qxm, https://www.itophub.io/wiki/page?id=2_7_0%3Arelease%3Achange_log	A-COM-ITOP-060820/118
Improper	05-06-2020	4.3	In Combodo iTop, dashboard	https://gith	A-COM-ITOP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			ids can be exploited with a reflective XSS payload. This is fixed in all iTop packages (community, essential, professional) for version 2.7.0 and in iTop essential and iTop professional packages for version 2.6.4. **CVE ID : CVE-2020-11697**	ub.com/Combodo/iTop/security/advisories/GHSA-xfh9-5632-hxmv, https://www.itophub.io/wiki/page?id=2_7_0%3Arelease%3A2_7_whats_new	060820/119
connectwise					
automate_api					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-06-2020	6.5	By using an Automate API in ConnectWise Automate before 2020.5.178, a remote authenticated user could execute commands and/or modifications within an individual Automate instance by triggering an SQL injection vulnerability in /LabTech/agent.aspx. This affects versions before 2019.12.337, 2020 before 2020.1.53, 2020.2 before 2020.2.85, 2020.3 before 2020.3.114, 2020.4 before 2020.4.143, and 2020.5 before 2020.5.178. **CVE ID : CVE-2020-14159**	N/A	A-CON-AUTO-060820/120
couchbase					
couchbase_server					
Improper Resource Shutdown or Release	08-06-2020	5	In Couchbase Server 6.0.3 and Couchbase Sync Gateway through 2.7.0, the Cluster management, views,	https://www.couchbase.com/resources/secur	A-COU-COUC-060820/121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			query, and full-text search endpoints are vulnerable to the Slowloris denial-of-service attack because they don't more aggressively terminate slow connections. **CVE ID : CVE-2020-9041**	ity#Security Alerts	
Cross-Site Request Forgery (CSRF)	08-06-2020	6.8	In Couchbase Server 6.0, credentials cached by a browser can be used to perform a CSRF attack if an administrator has used their browser to check the results of a REST API request. **CVE ID : CVE-2020-9042**	https://www.couchbase.com/resources/security#Security Alerts	A-COU-COUC-060820/122
couchbase_server_java_sdk					
Improper Certificate Validation	08-06-2020	5	Couchbase Server Java SDK before 2.7.1.1 allows a potential attacker to forge an SSL certificate and pose as the intended peer. An attacker can leverage this flaw by crafting a cryptographically valid certificate that will be accepted by Java SDK's Netty component due to missing hostname verification. **CVE ID : CVE-2020-9040**	https://www.couchbase.com/resources/security#Security Alerts	A-COU-COUC-060820/123
sync_gateway					
Improper Resource Shutdown or Release	08-06-2020	5	In Couchbase Server 6.0.3 and Couchbase Sync Gateway through 2.7.0, the Cluster management, views, query, and full-text search endpoints are vulnerable to the Slowloris denial-of-service attack because they don't more aggressively	https://www.couchbase.com/resources/security#Security Alerts	A-COU-SYNC-060820/124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate slow connections. **CVE ID : CVE-2020-9041**		
Cypress					
psoc_4.2_ble					
Insufficient Entropy	09-06-2020	5.4	The Bluetooth Low Energy implementation in Cypress PSoC Creator BLE 4.2 component versions before 3.64 generates a random number (Pairing Random) with significantly less entropy than the specified 128 bits during BLE pairing. This is the case for both authenticated and unauthenticated pairing with both LE Secure Connections as well as LE Legacy Pairing. A predictable or brute-forceable random number allows an attacker (in radio range) to perform a MITM attack during BLE pairing. **CVE ID : CVE-2020-11957**	https://www.cypress.com/file/504466/download	A-CYP-PSOC-060820/125
Dell					
encryption					
Incorrect Permission Assignment for Critical Resource	15-06-2020	7.2	Dell Encryption versions prior to 10.7 and Dell Endpoint Security Suite versions prior to 2.7 contain a privilege escalation vulnerability due to incorrect permissions. A local malicious user with low privileges could potentially exploit this vulnerability to gain elevated privilege on the affected system with the	N/A	A-DEL-ENCR-060820/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			help of a symbolic link. **CVE ID : CVE-2020-5358**		
endpoint_security_suite_enterprise					
Incorrect Permission Assignment for Critical Resource	15-06-2020	7.2	Dell Encryption versions prior to 10.7 and Dell Endpoint Security Suite versions prior to 2.7 contain a privilege escalation vulnerability due to incorrect permissions. A local malicious user with low privileges could potentially exploit this vulnerability to gain elevated privilege on the affected system with the help of a symbolic link. **CVE ID : CVE-2020-5358**	N/A	A-DEL-ENDP-060820/127
dext5					
dext5					
Incorrect Default Permissions	07-06-2020	5	handler/upload_handler.jsp in DEXT5 Editor through 3.5.1402961 allows an attacker to download arbitrary files via the savefilepath field. **CVE ID : CVE-2020-13894**	N/A	A-DEX-DEXT-060820/128
digdash					
digdash					
Server-Side Request Forgery (SSRF)	15-06-2020	5	An issue was discovered in DigDash 2018R2 before p20200210 and 2019R1 before p20200210. The login page is vulnerable to Server-Side Request Forgery (SSRF) that allows use of the application as a proxy. Sent to an external server, a forged request discloses	N/A	A-DIG-DIGD-060820/129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application credentials. For a request to an internal component, the request is blind, but through the error message it's possible to determine whether the request targeted a open service. **CVE ID : CVE-2020-13650**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	15-06-2020	6.8	An issue was discovered in DigDash 2018R2 before p20200528, 2019R1 before p20200421, and 2019R2 before p20200430. It allows a user to provide data that will be used to generate the JNLP file used by a client to obtain the right Java application. By providing an attacker-controlled URL, the client will obtain a rogue JNLP file specifying the installation of malicious JAR archives and executed with full privileges on the client computer. **CVE ID : CVE-2020-13651**	N/A	A-DIG-DIGD-060820/130
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-06-2020	4.3	An issue was discovered in DigDash 2018R2 before p20200528, 2019R1 before p20200528, 2019R2 before p20200430, and 2020R1 before p20200507. A cross-site scripting (XSS) vulnerability exists in the login menu. **CVE ID : CVE-2020-13652**	N/A	A-DIG-DIGD-060820/131
Djangoproject					
django					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	03-06-2020	4.3	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. In cases where a memcached backend does not perform key validation, passing malformed cache keys could result in a key collision, and potential data leakage. **CVE ID : CVE-2020-13254**	https://security.netapp.com/advisory/ntap-20200611-0002/, https://www.djangoproject.com/weblog/2020/jun/03/security-releases/	A-DJA-DJAN-060820/132
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	4.3	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. Query parameters generated by the Django admin ForeignKeyRawIdWidget were not properly URL encoded, leading to a possibility of an XSS attack. **CVE ID : CVE-2020-13596**	https://security.netapp.com/advisory/ntap-20200611-0002/, https://www.djangoproject.com/weblog/2020/jun/03/security-releases/	A-DJA-DJAN-060820/133
Docker					
docker_desktop					
Improper Privilege Management	05-06-2020	7.2	An issue was discovered in Docker Desktop through 2.2.0.5 on Windows. If a local attacker sets up their own named pipe prior to starting Docker with the same name, this attacker can intercept a connection attempt from Docker Service (which runs as SYSTEM), and then impersonate their privileges.	N/A	A-DOC-DOCK-060820/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11492		
engine					
Improper Input Validation	02-06-2020	6	An issue was discovered in Docker Engine before 19.03.11. An attacker in a container, with the CAP_NET_RAW capability, can craft IPv6 router advertisements, and consequently spoof external IPv6 hosts, obtain sensitive information, or cause a denial of service. **CVE ID : CVE-2020-13401**	https://github.com/docker/docker-ce/releases/tag/v19.03.11, https://security.netapp.com/advisory/ntap-20200717-0002/	A-DOC-ENGI-060820/135
Elastic					
elastic_cloud_on_kubernetes					
Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	03-06-2020	5	Elastic Cloud on Kubernetes (ECK) versions prior to 1.1.0 generate passwords using a weak random number generator. If an attacker is able to determine when the current Elastic Stack cluster was deployed they may be able to more easily brute force the Elasticsearch credentials generated by ECK. **CVE ID : CVE-2020-7010**	N/A	A-ELA-ELAS-060820/136
elastic_app_search					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	4.3	Elastic App Search versions before 7.7.0 contain a cross site scripting (XSS) flaw when displaying document URLs in the Reference UI. If the Reference UI injects a URL into a result, that URL will be rendered by the web	N/A	A-ELA-ELAS-060820/137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			browser. If an attacker is able to control the contents of such a field, they could execute arbitrary JavaScript in the victimï¿½s web browser. **CVE ID : CVE-2020-7011**		
elasticsearch					
Improper Privilege Management	03-06-2020	6.5	The fix for CVE-2020-7009 was found to be incomplete. Elasticsearch versions from 6.7.0 to 6.8.7 and 7.0.0 to 7.6.1 contain a privilege escalation flaw if an attacker is able to create API keys and also authentication tokens. An attacker who is able to generate an API key and an authentication token can perform a series of steps that result in an authentication token being generated with elevated privileges. **CVE ID : CVE-2020-7014**	https://security.netapp.com/advisory/ntap-20200619-0003/	A-ELA-ELAS-060820/138
Elasticsearch					
kibana					
Improper Control of Generation of Code ('Code Injection')	03-06-2020	6.5	Kibana versions 6.7.0 to 6.8.8 and 7.0.0 to 7.6.2 contain a prototype pollution flaw in the Upgrade Assistant. An authenticated attacker with privileges to write to the Kibana index could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing	N/A	A-ELA-KIBA-060820/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code with the permissions of the Kibana process on the host system. **CVE ID : CVE-2020-7012**		
Improper Control of Generation of Code ('Code Injection')	03-06-2020	6.5	Kibana versions before 6.8.9 and 7.7.0 contain a prototype pollution flaw in TSVB. An authenticated attacker with privileges to create TSVB visualizations could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system. **CVE ID : CVE-2020-7013**	N/A	A-ELA-KIBA-060820/140
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	3.5	Kibana versions before 6.8.9 and 7.7.0 contains a stored XSS flaw in the TSVB visualization. An attacker who is able to edit or create a TSVB visualization could allow the attacker to obtain sensitive information from, or perform destructive actions, on behalf of Kibana users who edit the TSVB visualization. **CVE ID : CVE-2020-7015**	N/A	A-ELA-KIBA-060820/141
elementor					
elementor_page_builder					
Improper Neutralization of Input During Web Page Generation	05-06-2020	3.5	The Elementor Page Builder plugin before 2.9.9 for WordPress suffers from a stored XSS vulnerability. An author user can create posts that result in a stored XSS by	N/A	A-ELE-ELEM-060820/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			using a crafted payload in custom links. **CVE ID : CVE-2020-13864**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-06-2020	3.5	The Elementor Page Builder plugin before 2.9.9 for WordPress suffers from multiple stored XSS vulnerabilities. An author user can create posts that result in stored XSS vulnerabilities, by using a crafted link in the custom URL or by applying custom attributes. **CVE ID : CVE-2020-13865**	N/A	A-ELE-ELEM-060820/143
elliptic_project					
elliptic					
Integer Overflow or Wraparound	04-06-2020	6.8	The Elliptic package 6.5.2 for Node.js allows ECDSA signature malleability via variations in encoding, leading '\0' bytes, or integer overflows. This could conceivably have a security-relevant impact if an application relied on a single canonical signature. **CVE ID : CVE-2020-13822**	N/A	A-ELL-ELLI-060820/144
enhancesoft					
osticket					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-06-2020	3.5	scp/categories.php in osTicket 1.14.2 allows XSS via a Knowledgebase Category Name or Category Description. The attacker must be an Agent. **CVE ID : CVE-2020-14012**	N/A	A-ENH-OSTI-060820/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fastecdsa_project					
fastecdsa					
Improper Verification of Cryptographic Signature	02-06-2020	5	An issue was discovered in fastecdsa before 2.1.2. When using the NIST P-256 curve in the ECDSA implementation, the point at infinity is mishandled. This means that for an extreme value in k and s^-1, the signature verification fails even if the signature is correct. This behavior is not solely a usability problem. There are some threat models where an attacker can benefit by successfully guessing users for whom signature verification will fail. **CVE ID : CVE-2020-12607**	https://github.com/AntonKueltz/fastecdsa/commit/4a16daeaf139be20654ef58a9fe4c79dc030458c, https://github.com/AntonKueltz/fastecdsa/commit/7b64e3efaa806b4daaf73bb5172af3581812f8de, https://github.com/AntonKueltz/fastecdsa/issues/52	A-FAS-FAST-060820/146
Fasterxml					
jackson-databind					
Deserialization of Untrusted Data	14-06-2020	6.8	FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to oadd.org.apache.xalan.lib.sql.JNDIConnectionPool (aka apache/drill). **CVE ID : CVE-2020-14060**	https://security.netapp.com/advisory/ntap-20200702-0003/	A-FAS-JACK-060820/147
Deserialization of	14-06-2020	6.8	FasterXML jackson-databind 2.x before 2.9.10.5	https://security.netap	A-FAS-JACK-060820/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			mishandles the interaction between serialization gadgets and typing, related to oracle.jms.AQjmsQueueConnectionFactory, oracle.jms.AQjmsXATopicConnectionFactory, oracle.jms.AQjmsTopicConnectionFactory, oracle.jms.AQjmsXAQueueConnectionFactory, and oracle.jms.AQjmsXAConnectionFactory (aka weblogic/oracle-aqjms). **CVE ID : CVE-2020-14061**	p.com/advisory/ntap-20200702-0003/	
Deserialization of Untrusted Data	14-06-2020	6.8	FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to com.sun.org.apache.xalan.internal.lib.sql.JNDIConnectionPool (aka xalan2). **CVE ID : CVE-2020-14062**	https://security.netapp.com/advisory/ntap-20200702-0003/	A-FAS-JACK-060820/149
Ffmpeg					
ffmpeg					
Use After Free	07-06-2020	4.3	FFmpeg 4.2.3 has a use-after-free via a crafted EXTINF duration in an m3u8 file because parse_playlist in libavformat/hls.c frees a pointer, and later that pointer is accessed in av_probe_input_format3 in libavformat/format.c. **CVE ID : CVE-2020-13904**	N/A	A-FFM-FFMP-060820/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Fortinet					
fortisiem_windows_agent					
Unquoted Search Path or Element	04-06-2020	7.5	An unquoted service path vulnerability in the FortiSIEM Windows Agent component may allow an attacker to gain elevated privileges via the AoWinAgt executable service path. **CVE ID : CVE-2020-9292**	N/A	A-FOR-FORT-060820/151
fortianalyzer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-06-2020	3.5	An improper neutralization of input vulnerability in the Admin Profile of FortiAnalyzer may allow a remote authenticated attacker to perform a stored cross site scripting attack (XSS) via the Description Area. **CVE ID : CVE-2020-6640**	N/A	A-FOR-FORT-060820/152
forticlient					
Exposure of Resource to Wrong Sphere	01-06-2020	4.6	An Insecure Temporary File vulnerability in FortiClient for Windows 6.2.1 and below may allow a local user to gain elevated privileges via exhausting the pool of temporary file names combined with a symbolic link attack. **CVE ID : CVE-2020-9291**	N/A	A-FOR-FORT-060820/153
Foxitsoftware					
foxit_studio_photo					
Out-of-bounds Write	04-06-2020	6.8	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It has an out-of-	https://www.foxitsoftware.com/s	A-FOX-FOXI-060820/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bounds write via a crafted TIFF file. **CVE ID : CVE-2020-13811**	upport/security-bulletins.php	
Untrusted Search Path	04-06-2020	4.4	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It allows local users to gain privileges via a crafted DLL in the current working directory. **CVE ID : CVE-2020-13812**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-060820/155
Untrusted Search Path	04-06-2020	4.4	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It allows local users to gain privileges via a crafted DLL in the current working directory when FoxitStudioPhoto366_3.6.6.916.exe is used. **CVE ID : CVE-2020-13813**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-060820/156
phantompdf					
Improper Verification of Cryptographic Signature	04-06-2020	5	An issue was discovered in Foxit PhantomPDF Mac and Foxit Reader for Mac before 4.0. It allows signature validation bypass via a modified file or a file with non-standard signatures. **CVE ID : CVE-2020-13803**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-060820/157
Use of Hard-coded Credentials	04-06-2020	6.8	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows information disclosure of a hardcoded username and password in the DocuSign plugin. **CVE ID : CVE-2020-13804**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-060820/158
Improper	04-06-2020	5	An issue was discovered in	https://ww	A-FOX-PHAN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Excessive Authenticati on Attempts			Foxit Reader and PhantomPDF before 9.7.2. It has brute-force attack mishandling because the CAS service lacks a limit on login failures. **CVE ID : CVE-2020-13805**	w.foxitsoft ware.com/s upport/sec urity-bulletins.ph p	060820/159
Uncontrolled Resource Consumption	04-06-2020	5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has a use-after-free because of JavaScript execution after a deletion or close operation. **CVE ID : CVE-2020-13806**	https://ww w.foxitsoft ware.com/s upport/sec urity-bulletins.ph p	A-FOX-PHAN-060820/160
Loop with Unreachable Exit Condition ('Infinite Loop')	04-06-2020	5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has circular reference mishandling that causes a loop. **CVE ID : CVE-2020-13807**	https://ww w.foxitsoft ware.com/s upport/sec urity-bulletins.ph p	A-FOX-PHAN-060820/161
Uncontrolled Resource Consumption	04-06-2020	5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows resource consumption via crafted cross-reference stream data. **CVE ID : CVE-2020-13808**	https://ww w.foxitsoft ware.com/s upport/sec urity-bulletins.ph p	A-FOX-PHAN-060820/162
Uncontrolled Resource Consumption	04-06-2020	5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows resource consumption via long strings in the content stream. **CVE ID : CVE-2020-13809**	https://ww w.foxitsoft ware.com/s upport/sec urity-bulletins.ph p	A-FOX-PHAN-060820/163
Improper Verification of	04-06-2020	5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It	https://ww w.foxitsoft ware.com/s	A-FOX-PHAN-060820/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Signature			allows signature validation bypass via a modified file or a file with non-standard signatures. **CVE ID : CVE-2020-13810**	upport/security-bulletins.php	
Use After Free	04-06-2020	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.1. It has a use-after-free via a document that lacks a dictionary. **CVE ID : CVE-2020-13814**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-060820/165
Uncontrolled Resource Consumption	04-06-2020	5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.1. It allows stack consumption via a loop of an indirect object reference. **CVE ID : CVE-2020-13815**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-060820/166
reader					
Improper Verification of Cryptographic Signature	04-06-2020	5	An issue was discovered in Foxit PhantomPDF Mac and Foxit Reader for Mac before 4.0. It allows signature validation bypass via a modified file or a file with non-standard signatures. **CVE ID : CVE-2020-13803**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-READ-060820/167
Use of Hard-coded Credentials	04-06-2020	6.8	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows information disclosure of a hardcoded username and password in the DocuSign plugin. **CVE ID : CVE-2020-13804**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-READ-060820/168
Improper Restriction	04-06-2020	5	An issue was discovered in Foxit Reader and	https://www.foxitsoft	A-FOX-READ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Excessive Authenticati on Attempts			PhantomPDF before 9.7.2. It has brute-force attack mishandling because the CAS service lacks a limit on login failures. **CVE ID : CVE-2020-13805**	ware.com/s upport/sec urity-bulletins.ph p	060820/169
Uncontrolled Resource Consumption	04-06-2020	5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has a use-after-free because of JavaScript execution after a deletion or close operation. **CVE ID : CVE-2020-13806**	https://ww w.foxitsoft ware.com/s upport/sec urity-bulletins.ph p	A-FOX-READ-060820/170
Loop with Unreachable Exit Condition ('Infinite Loop')	04-06-2020	5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has circular reference mishandling that causes a loop. **CVE ID : CVE-2020-13807**	https://ww w.foxitsoft ware.com/s upport/sec urity-bulletins.ph p	A-FOX-READ-060820/171
Uncontrolled Resource Consumption	04-06-2020	5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows resource consumption via crafted cross-reference stream data. **CVE ID : CVE-2020-13808**	https://ww w.foxitsoft ware.com/s upport/sec urity-bulletins.ph p	A-FOX-READ-060820/172
Uncontrolled Resource Consumption	04-06-2020	5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows resource consumption via long strings in the content stream. **CVE ID : CVE-2020-13809**	https://ww w.foxitsoft ware.com/s upport/sec urity-bulletins.ph p	A-FOX-READ-060820/173
Improper Verification of Cryptographi	04-06-2020	5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows signature validation	https://ww w.foxitsoft ware.com/s upport/sec	A-FOX-READ-060820/174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c Signature			bypass via a modified file or a file with non-standard signatures. **CVE ID : CVE-2020-13810**	urity-bulletins.php	
Use After Free	04-06-2020	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.1. It has a use-after-free via a document that lacks a dictionary. **CVE ID : CVE-2020-13814**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-READ-060820/175
Uncontrolled Resource Consumption	04-06-2020	5	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.1. It allows stack consumption via a loop of an indirect object reference. **CVE ID : CVE-2020-13815**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-READ-060820/176
Freedesktop					
systemd					
Improper Input Validation	03-06-2020	6.2	systemd through v245 mishandles numerical usernames such as ones composed of decimal digits or 0x followed by hex digits, as demonstrated by use of root privileges when privileges of the 0x0 user account were intended. NOTE: this issue exists because of an incomplete fix for CVE-2017-1000082. **CVE ID : CVE-2020-13776**	https://security.netapp.com/advisory/ntap-20200611-0003/	A-FRE-SYST-060820/177
dbus					
Improper Resource Shutdown or	08-06-2020	4.9	An issue was discovered in dbus >= 1.3.0 before 1.12.18. The DBusServer in libdbus, as used in dbus-daemon,	http://www.openwall.com/lists/oss-	A-FRE-DBUS-060820/178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Release			leaks file descriptors when a message exceeds the per-message file descriptor limit. A local attacker with access to the D-Bus system bus or another system service's private AF_UNIX socket could use this to make the system service reach its file descriptor limit, denying service to subsequent D-Bus clients. **CVE ID : CVE-2020-12049**	security/2020/06/04/3	
gesio					
erp					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-06-2020	7.5	There is an improper Neutralization of Special Elements used in an SQL Command (SQL Injection) vulnerability in php files of GESIO ERP. GESIO ERP all versions prior to 11.2 allows malicious users to retrieve all database information. **CVE ID : CVE-2020-8967**	https://www.incibe-cert.es/en/early-warning/security-advisories/gesio-sql-injection-vulnerability	A-GES-ERP-060820/179
Github					
github					
Files or Directories Accessible to External Parties	03-06-2020	7.5	An improper access control vulnerability was identified in the GitHub Enterprise Server API that allowed an organization member to escalate permissions and gain access to unauthorized repositories within an organization. This vulnerability affected all versions of GitHub	N/A	A-GIT-GITH-060820/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Server prior to 2.21 and was fixed in 2.20.9, 2.19.15, and 2.18.20. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2020-10516**		
Gitlab					
gitlab					
Missing Authorization	09-06-2020	4	Insecure authorization in Project Deploy Keys in GitLab CE/EE 12.8 and later through 13.0.1 allows users to update permissions of other users' deploy keys under certain conditions **CVE ID : CVE-2020-13266**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13266.json	A-GIT-GITL-060820/181
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-06-2020	4.3	A Stored Cross-Site Scripting vulnerability allowed the execution on Javascript payloads on the Metrics Dashboard in GitLab CE/EE 12.8 and later through 13.0.1 **CVE ID : CVE-2020-13267**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13267.json	A-GIT-GITL-060820/182
Improper Input Validation	10-06-2020	5	A specially crafted request could be used to confirm the existence of files hosted on object storage services, without disclosing their contents. This vulnerability affects GitLab CE/EE 12.10 and later through 13.0.1 **CVE ID : CVE-2020-13268**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13268.json	A-GIT-GITL-060820/183
Improper Neutralization of Input During Web	10-06-2020	4.3	A Reflected Cross-Site Scripting vulnerability allowed the execution of arbitrary Javascript code on	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-060820/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			the Static Site Editor in GitLab CE/EE 12.10 and later through 13.0.1 **CVE ID : CVE-2020-13269**	/blob/master/2020/CVE-2020-13269.json	
Incorrect Default Permissions	10-06-2020	6.5	Missing permission check on fork relation creation in GitLab CE/EE 11.3 and later through 13.0.1 allows guest users to create a fork relation on restricted public projects via API **CVE ID : CVE-2020-13270**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13270.json	A-GIT-GITL-060820/185
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-06-2020	4.3	A Stored Cross-Site Scripting vulnerability allowed the execution of arbitrary Javascript code in the blobs API in all previous GitLab CE/EE versions through 13.0.1 **CVE ID : CVE-2020-13271**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13271.json	A-GIT-GITL-060820/186
Gnome					
networkmanager					
Improper Authentication	08-06-2020	4	It was found that nmcli, a command line interface to NetworkManager did not honour 802-1x.ca-path and 802-1x.phase2-ca-path settings, when creating a new profile. When a user connects to a network using this profile, the authentication does not happen and the connection is made insecurely. **CVE ID : CVE-2020-10754**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10754	A-GNO-NETW-060820/187
GNU					
bison					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	15-06-2020	2.1	GNU Bison before 3.5.4 allows attackers to cause a denial of service (application crash). **CVE ID : CVE-2020-14150**	N/A	A-GNU-BISO-060820/188
gnutls					
Use of a Broken or Risky Cryptographic Algorithm	04-06-2020	5.8	GnuTLS 3.6.x before 3.6.14 uses incorrect cryptography for encrypting a session ticket (a loss of confidentiality in TLS 1.2, and an authentication bypass in TLS 1.3). The earliest affected version is 3.6.4 (2018-09-24) because of an error in a 2018-09-18 commit. Until the first key rotation, the TLS server always uses wrong data in place of an encryption key derived from an application. **CVE ID : CVE-2020-13777**	https://gnutls.org/security-new.html#GNUTLS-SA-2020-06-03, https://security.netapp.com/advisory/ntap-20200619-0004/	A-GNU-GNUT-060820/189
goliath_project					
goliath					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	10-06-2020	5	goliath through 1.0.6 allows request smuggling attacks where goliath is used as a backend and a frontend proxy also being vulnerable. It is possible to conduct HTTP request smuggling attacks by sending the Content-Length header twice. Furthermore, invalid Transfer Encoding headers were found to be parsed as valid which could be leveraged for TE:CL smuggling attacks.	N/A	A-GOL-GOLI-060820/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7671		
Google					
chrome					
Out-of-bounds Write	03-06-2020	6.8	Out of bounds write in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6419**	N/A	A-GOO-CHRO-060820/191
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	6.8	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6453**	N/A	A-GOO-CHRO-060820/192
Use After Free	03-06-2020	6.8	Use after free in WebAuthentication in Google Chrome prior to 83.0.4103.97 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2020-6493**	N/A	A-GOO-CHRO-060820/193
Improper Input Validation	03-06-2020	4.3	Incorrect security UI in payments in Google Chrome on Android prior to 83.0.4103.97 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	N/A	A-GOO-CHRO-060820/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6494		
Incorrect Default Permissions	03-06-2020	4.3	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.97 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. **CVE ID : CVE-2020-6495**	N/A	A-GOO-CHRO-060820/195
Use After Free	03-06-2020	6.8	Use after free in payments in Google Chrome on MacOS prior to 83.0.4103.97 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2020-6496**	N/A	A-GOO-CHRO-060820/196
Incorrect Default Permissions	03-06-2020	4.3	Insufficient policy enforcement in Omnibox in Google Chrome on iOS prior to 83.0.4103.88 allowed a remote attacker to perform domain spoofing via a crafted URI. **CVE ID : CVE-2020-6497**	N/A	A-GOO-CHRO-060820/197
Incorrect Default Permissions	03-06-2020	4.3	Incorrect implementation in user interface in Google Chrome on iOS prior to 83.0.4103.88 allowed a remote attacker to perform domain spoofing via a crafted HTML page. **CVE ID : CVE-2020-6498**	N/A	A-GOO-CHRO-060820/198
N/A	03-06-2020	4.3	Inappropriate implementation in AppCache	N/A	A-GOO-CHRO-060820/199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass AppCache security restrictions via a crafted HTML page. **CVE ID : CVE-2020-6499**		
N/A	03-06-2020	4.3	Inappropriate implementation in interstitials in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2020-6500**	N/A	A-GOO-CHRO-060820/200
Incorrect Default Permissions	03-06-2020	4.3	Insufficient policy enforcement in CSP in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2020-6501**	N/A	A-GOO-CHRO-060820/201
Incorrect Default Permissions	03-06-2020	4.3	Incorrect implementation in permissions in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof security UI via a crafted HTML page. **CVE ID : CVE-2020-6502**	N/A	A-GOO-CHRO-060820/202
Information Exposure	03-06-2020	4.3	Inappropriate implementation in accessibility in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain	N/A	A-GOO-CHRO-060820/203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially sensitive information from process memory via a crafted HTML page. **CVE ID : CVE-2020-6503**		
Incorrect Default Permissions	03-06-2020	4.3	Insufficient policy enforcement in notifications in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass notification restrictions via a crafted HTML page. **CVE ID : CVE-2020-6504**	N/A	A-GOO-CHRO-060820/204
grafana					
grafana					
Server-Side Request Forgery (SSRF)	03-06-2020	6.4	The avatar feature in Grafana 3.0.1 through 7.0.1 has an SSRF Incorrect Access Control issue. This vulnerability allows any unauthenticated user/client to make Grafana send HTTP requests to any URL and return its result to the user/client. This can be used to gain information about the network that Grafana is running on. Furthermore, passing invalid URL objects could be used for DOS'ing Grafana via SegFault. **CVE ID : CVE-2020-13379**	http://www.openwall.com/lists/oss-security/2020/06/03/4, https://grafana.com/blog/2020/06/03/grafana-6.7.4-and-7.0.2-released-with-important-security-fix/, https://security.netapp.com/advisory/ntap-20200608-0006/	A-GRA-GRAF-060820/205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
hashicorp					
consul					
Improper Input Validation	11-06-2020	5	HashiCorp Consul and Consul Enterprise did not appropriately enforce scope for local tokens issued by a primary data center, where replication to a secondary data center was not enabled. Introduced in 1.4.0, fixed in 1.6.6 and 1.7.4. **CVE ID : CVE-2020-13170**	https://github.com/hashicorp/consul/blob/v1.6.6/CHANGELOG.md, https://github.com/hashicorp/consul/blob/v1.7.4/CHANGELOG.md, https://github.com/hashicorp/consul/pull/8068	A-HAS-CONS-060820/206
Improper Resource Shutdown or Release	11-06-2020	5	HashiCorp Consul and Consul Enterprise could crash when configured with an abnormally-formed service-router entry. Introduced in 1.6.0, fixed in 1.6.6 and 1.7.4. **CVE ID : CVE-2020-12758**	https://github.com/hashicorp/consul/blob/v1.6.6/CHANGELOG.md, https://github.com/hashicorp/consul/blob/v1.7.4/CHANGELOG.md, https://github.com/hashicorp/consul/pull/7783	A-HAS-CONS-060820/207
Incorrect Permission Assignment for Critical	11-06-2020	5	HashiCorp Consul and Consul Enterprise failed to enforce changes to legacy ACL token rules due to non-	https://github.com/hashicorp/consul/blob/v1.	A-HAS-CONS-060820/208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource			propagation to secondary data centers. Introduced in 1.4.0, fixed in 1.6.6 and 1.7.4. **CVE ID : CVE-2020-12797**	6.6/CHANGELOG.md, https://github.com/hashicorp/consul/blob/v1.7.4/CHANGELOG.md, https://github.com/hashicorp/consul/pull/8047	
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-06-2020	5	HashiCorp Consul and Consul Enterprise include an HTTP API (introduced in 1.2.0) and DNS (introduced in 1.4.3) caching feature that was vulnerable to denial of service. Fixed in 1.6.6 and 1.7.4. **CVE ID : CVE-2020-13250**	https://github.com/hashicorp/consul/blob/v1.6.6/CHANGELOG.md, https://github.com/hashicorp/consul/blob/v1.7.4/CHANGELOG.md, https://github.com/hashicorp/consul/pull/8023	A-HAS-CONS-060820/209
vault					
Information Exposure	10-06-2020	5	HashiCorp Vault and Vault Enterprise before 1.3.6, and 1.4.2 before 1.4.2, insert Sensitive Information into a Log File. **CVE ID : CVE-2020-13223**	N/A	A-HAS-VAUL-060820/210
Improper Privilege	10-06-2020	7.5	HashiCorp Vault and Vault Enterprise 1.4.x before 1.4.2	https://www.hashicorp.com/blog/	A-HAS-VAUL-060820/211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			has Incorrect Access Control. **CVE ID : CVE-2020-12757**	category/vault/	
hcltech					
hcl_digital_experience					
Server-Side Request Forgery (SSRF)	11-06-2020	7.5	"HCL Digital Experience is susceptible to Server Side Request Forgery." **CVE ID : CVE-2020-4101**	N/A	A-HCL-HCL_-060820/212
Hesk					
hesk					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-06-2020	4.3	HESK before 3.1.10 allows reflected XSS. **CVE ID : CVE-2020-13897**	N/A	A-HES-HESK-060820/213
Huawei					
fusionaccess					
Improper Input Validation	15-06-2020	4	FusionAccess with versions earlier than 6.5.1.SPC002 have a Denial of Service (DoS) vulnerability. Due to insufficient verification on specific input, attackers can exploit this vulnerability by sending constructed messages to the affected device through another device on the same network. Successful exploit could cause affected devices to be abnormal. **CVE ID : CVE-2020-1825**	N/A	A-HUA-FUSI-060820/214
IBM					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
planning_analytics_local					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-06-2020	3.5	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178765. **CVE ID : CVE-2020-4360**	https://www.ibm.com/support/pages/node/6214472	A-IBM-PLAN-060820/215
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-06-2020	4.3	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178965. **CVE ID : CVE-2020-4366**	https://www.ibm.com/support/pages/node/6214472	A-IBM-PLAN-060820/216
Use of a Broken or Risky Cryptographic Algorithm	02-06-2020	5	IBM Planning Analytics Local 2.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 179001. **CVE ID : CVE-2020-4367**	https://www.ibm.com/support/pages/node/6214472	A-IBM-PLAN-060820/217
Improper Neutralization of Input During Web	02-06-2020	3.5	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to	https://www.ibm.com/support/pages/node/6	A-IBM-PLAN-060820/218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 180761. **CVE ID : CVE-2020-4431**	214472	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-06-2020	4.3	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 182283. **CVE ID : CVE-2020-4503**	https://www.ibm.com/support/pages/node/6214472	A-IBM-PLAN-060820/219
security_guardium					
Use of Hard-coded Credentials	03-06-2020	7.5	IBM Security Guardium 11.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174732. **CVE ID : CVE-2020-4177**	https://www.ibm.com/support/pages/node/6218970	A-IBM-SECU-060820/220
Improper Neutralization of Special Elements used in an OS	03-06-2020	9	IBM Security Guardium 11.1 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a	https://www.ibm.com/support/pages/node/6218960	A-IBM-SECU-060820/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 174735. **CVE ID : CVE-2020-4180**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	4.3	IBM Security Guardium 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174738. **CVE ID : CVE-2020-4182**	https://www.ibm.com/support/pages/node/6218964	A-IBM-SECU-060820/222
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-06-2020	4.3	IBM Security Guardium 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174739. **CVE ID : CVE-2020-4183**	https://www.ibm.com/support/pages/node/6220126	A-IBM-SECU-060820/223
Information Exposure	03-06-2020	5	IBM Security Guardium 11.1 could disclose sensitive information on the login page that could aid in further attacks against the system. IBM X-Force ID: 174805. **CVE ID : CVE-2020-4187**	https://www.ibm.com/support/pages/node/6218972	A-IBM-SECU-060820/224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	03-06-2020	4.6	IBM Security Guardium 10.6, 11.0, and 11.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174851. **CVE ID : CVE-2020-4190**	https://www.ibm.com/support/pages/node/6218958	A-IBM-SECU-060820/225
Use of a Broken or Risky Cryptographic Algorithm	04-06-2020	2.1	IBM Security Guardium 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174852. **CVE ID : CVE-2020-4191**	https://www.ibm.com/support/pages/node/6220130	A-IBM-SECU-060820/226
Improper Restriction of Excessive Authentication Attempts	04-06-2020	5	IBM Security Guardium 11.1 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 174857. **CVE ID : CVE-2020-4193**	https://www.ibm.com/support/pages/node/6220132	A-IBM-SECU-060820/227
Improper Privilege Management	03-06-2020	3.3	IBM Security Guardium 11.1 could allow an attacker on the same network to gain access to the Solr dashboard and cause a denial of service attack. IBM X-Force ID: 176997. **CVE ID : CVE-2020-4307**	https://www.ibm.com/support/pages/node/6218974	A-IBM-SECU-060820/228
spectrum_protect_plus					
Use of Hard-coded	15-06-2020	7.5	IBM Spectrum Protect Plus 10.1.0 through 10.1.5	https://www.ibm.com/	A-IBM-SPEC-060820/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 175066. **CVE ID : CVE-2020-4216**	support/pages/node/6221332	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	15-06-2020	10	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. This vulnerability is due to an incomplete fix for CVE-2020-4211. IBM X-Force ID: 181724. **CVE ID : CVE-2020-4469**	https://www.ibm.com/support/pages/node/6221358	A-IBM-SPEC-060820/230
Unrestricted Upload of File with Dangerous Type	15-06-2020	6	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 Administrative Console could allow an authenticated attacker to upload arbitrary files which could be execute arbitrary code on the vulnerable server. IBM X-Force ID: 181725. **CVE ID : CVE-2020-4470**	https://www.ibm.com/support/pages/node/6221358	A-IBM-SPEC-060820/231
Improper Input Validation	15-06-2020	6.4	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow an unauthenticated attacker to cause a denial of	https://www.ibm.com/support/pages/node/6	A-IBM-SPEC-060820/232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service or hijack DNS sessions by send a specially crafted HTTP command to the remote server. IBM X-Force ID: 181726. **CVE ID : CVE-2020-4471**	221358	
Information Exposure	15-06-2020	4	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 discloses highly sensitive information in plain text in the virgo log file which could be used in further attacks against the system. IBM X-Force ID: 181779. **CVE ID : CVE-2020-4477**	https://www.ibm.com/support/pages/node/6221388	A-IBM-SPEC-060820/233
mobile_foundation					
Session Fixation	05-06-2020	7.5	IBM Worklight/MobileFoundation 8.0.0.0 does not properly invalidate session cookies when a user logs out of a session, which could allow another user to gain unauthorized access to a user's session. IBM X-Force ID: 175211. **CVE ID : CVE-2020-4229**	https://www.ibm.com/support/pages/node/6220230	A-IBM-MOBI-060820/234
workload_scheduler					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-06-2020	3.5	IBM Workload Scheduler 9.3.0.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID:	https://www.ibm.com/support/pages/node/6223030	A-IBM-WORK-060820/235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			179160. **CVE ID : CVE-2020-4380**		
spectrum_protect_client					
Improper Restriction of Rendered UI Layers or Frames	15-06-2020	3.5	IBM Spectrum Protect Client 8.1.7.0 through 8.1.9.1 (Linux and Windows), 8.1.9.0 trough 8.1.9.1 (AIX) and IBM Spectrum Protect for Space Management 8.1.7.0 through 8.1.9.1 (Linux), 8.1.9.0 through 8.1.9.1 (AIX) web user interfaces could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 179488. **CVE ID : CVE-2020-4406**	https://www.ibm.com/support/pages/node/6221448	A-IBM-SPEC-060820/236
Information Exposure	15-06-2020	5	IBM Spectrum Protect Client 8.1.7.0 through 8.1.9.1 (Linux and Windows), 8.1.9.0 trough 8.1.9.1 (AIX) and IBM Spectrum Protect for Space Management 8.1.7.0 through 8.1.9.1 (Linux), 8.1.9.0 through 8.1.9.1 (AIX) web user interfaces could allow an attacker to bypass authentication due to improper session validation which can result in access to unauthorized resources. IBM	https://www.ibm.com/support/pages/node/6221448	A-IBM-SPEC-060820/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			X-Force ID: 182019. **CVE ID : CVE-2020-4494**		
spectrum_protect_for_space_management					
Improper Restriction of Rendered UI Layers or Frames	15-06-2020	3.5	IBM Spectrum Protect Client 8.1.7.0 through 8.1.9.1 (Linux and Windows), 8.1.9.0 trough 8.1.9.1 (AIX) and IBM Spectrum Protect for Space Management 8.1.7.0 through 8.1.9.1 (Linux), 8.1.9.0 through 8.1.9.1 (AIX) web user interfaces could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 179488. **CVE ID : CVE-2020-4406**	https://www.ibm.com/support/pages/node/6221448	A-IBM-SPEC-060820/238
Information Exposure	15-06-2020	5	IBM Spectrum Protect Client 8.1.7.0 through 8.1.9.1 (Linux and Windows), 8.1.9.0 trough 8.1.9.1 (AIX) and IBM Spectrum Protect for Space Management 8.1.7.0 through 8.1.9.1 (Linux), 8.1.9.0 through 8.1.9.1 (AIX) web user interfaces could allow an attacker to bypass authentication due to improper session validation which can result in access to unauthorized resources. IBM	https://www.ibm.com/support/pages/node/6221448	A-IBM-SPEC-060820/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			X-Force ID: 182019. **CVE ID : CVE-2020-4494**		
aspera_application_platform_on_demand					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to command injection after valid authentication, which could allow an attacker with intimate knowledge of the system to execute commands in a SOAP API. IBM X-Force ID: 180810. **CVE ID : CVE-2020-4432**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/240
Out-of-bounds Write	10-06-2020	9.3	Certain IBM Aspera applications are vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker with intimate knowledge of the server to execute arbitrary code on the system with the privileges of root or cause server to crash. IBM X-Force ID: 180814. **CVE ID : CVE-2020-4433**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/241
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow based on the product configuration and valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: 180900. **CVE ID : CVE-2020-4434**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-06-2020	6	Certain IBM Aspera applications are vulnerable to arbitrary memory corruption based on the product configuration, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180901. **CVE ID : CVE-2020-4435**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/243
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow after valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code through a service. IBM X-Force ID: 180902. **CVE ID : CVE-2020-4436**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/244
aspera_faspex_on_demand					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to command injection after valid authentication, which could allow an attacker with intimate knowledge of the system to execute commands in a SOAP API. IBM X-Force ID: 180810. **CVE ID : CVE-2020-4432**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/245
Out-of-bounds	10-06-2020	9.3	Certain IBM Aspera applications are vulnerable	https://www.ibm.com/	A-IBM-ASPE-060820/246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker with intimate knowledge of the server to execute arbitrary code on the system with the privileges of root or cause server to crash. IBM X-Force ID: 180814. **CVE ID : CVE-2020-4433**	support/pages/node/6221324	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow based on the product configuration and valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180900. **CVE ID : CVE-2020-4434**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/247
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-06-2020	6	Certain IBM Aspera applications are vulnerable to arbitrary memory corruption based on the product configuration, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180901. **CVE ID : CVE-2020-4435**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow after valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code through a service. IBM X-Force ID: 180902. **CVE ID : CVE-2020-4436**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/249
aspera_high-speed_transfer_endpoint					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to command injection after valid authentication, which could allow an attacker with intimate knowledge of the system to execute commands in a SOAP API. IBM X-Force ID: 180810. **CVE ID : CVE-2020-4432**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/250
Out-of-bounds Write	10-06-2020	9.3	Certain IBM Aspera applications are vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker with intimate knowledge of the server to execute arbitrary code on the system with the privileges of root or cause server to crash. IBM X-Force ID: 180814. **CVE ID : CVE-2020-4433**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/251
Buffer Copy without Checking Size of Input	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow based on the product configuration	https://www.ibm.com/support/pages/node/6	A-IBM-ASPE-060820/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			and valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180900. **CVE ID : CVE-2020-4434**	221324	
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-06-2020	6	Certain IBM Aspera applications are vulnerable to arbitrary memory corruption based on the product configuration, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180901. **CVE ID : CVE-2020-4435**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/253
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow after valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code through a service. IBM X-Force ID: 180902. **CVE ID : CVE-2020-4436**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/254
aspera_high-speed_transfer_server					
Improper Neutralization of Special Elements in Output Used	10-06-2020	6	Certain IBM Aspera applications are vulnerable to command injection after valid authentication, which could allow an attacker with	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream Component ('Injection')			intimate knowledge of the system to execute commands in a SOAP API. IBM X-Force ID: 180810. **CVE ID : CVE-2020-4432**		
Out-of-bounds Write	10-06-2020	9.3	Certain IBM Aspera applications are vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker with intimate knowledge of the server to execute arbitrary code on the system with the privileges of root or cause server to crash. IBM X-Force ID: 180814. **CVE ID : CVE-2020-4433**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/256
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow based on the product configuration and valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180900. **CVE ID : CVE-2020-4434**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/257
Improper Restriction of Operations within the Bounds of a	10-06-2020	6	Certain IBM Aspera applications are vulnerable to arbitrary memory corruption based on the product configuration, which could allow an attacker with	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180901. **CVE ID : CVE-2020-4435**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow after valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code through a service. IBM X-Force ID: 180902. **CVE ID : CVE-2020-4436**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/259
aspera_high-speed_transfer_server_for_cloud_pak_for_integration					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to command injection after valid authentication, which could allow an attacker with intimate knowledge of the system to execute commands in a SOAP API. IBM X-Force ID: 180810. **CVE ID : CVE-2020-4432**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/260
Out-of-bounds Write	10-06-2020	9.3	Certain IBM Aspera applications are vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker with intimate knowledge of the server to execute arbitrary code on the system with the privileges of root or cause	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server to crash. IBM X-Force ID: 180814. **CVE ID : CVE-2020-4433**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow based on the product configuration and valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180900. **CVE ID : CVE-2020-4434**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/262
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-06-2020	6	Certain IBM Aspera applications are vulnerable to arbitrary memory corruption based on the product configuration, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180901. **CVE ID : CVE-2020-4435**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/263
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow after valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code through a service. IBM X-Force ID: 180902.	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4436		
aspera_proxy_server					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to command injection after valid authentication, which could allow an attacker with intimate knowledge of the system to execute commands in a SOAP API. IBM X-Force ID: 180810. **CVE ID : CVE-2020-4432**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/265
Out-of-bounds Write	10-06-2020	9.3	Certain IBM Aspera applications are vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker with intimate knowledge of the server to execute arbitrary code on the system with the privileges of root or cause server to crash. IBM X-Force ID: 180814. **CVE ID : CVE-2020-4433**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/266
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow based on the product configuration and valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180900.	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4434		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-06-2020	6	Certain IBM Aspera applications are vulnerable to arbitrary memory corruption based on the product configuration, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180901. **CVE ID : CVE-2020-4435**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/268
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow after valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code through a service. IBM X-Force ID: 180902. **CVE ID : CVE-2020-4436**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/269
aspera_server_on_demand					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to command injection after valid authentication, which could allow an attacker with intimate knowledge of the system to execute commands in a SOAP API. IBM X-Force ID: 180810. **CVE ID : CVE-2020-4432**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/270
Out-of-bounds Write	10-06-2020	9.3	Certain IBM Aspera applications are vulnerable to a stack-based buffer overflow, caused by	https://www.ibm.com/support/pages/node/6	A-IBM-ASPE-060820/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper bounds checking. This could allow a remote attacker with intimate knowledge of the server to execute arbitrary code on the system with the privileges of root or cause server to crash. IBM X-Force ID: 180814. **CVE ID : CVE-2020-4433**	221324	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow based on the product configuration and valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180900. **CVE ID : CVE-2020-4434**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/272
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-06-2020	6	Certain IBM Aspera applications are vulnerable to arbitrary memory corruption based on the product configuration, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180901. **CVE ID : CVE-2020-4435**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/273
Buffer Copy without	10-06-2020	6	Certain IBM Aspera applications are vulnerable	https://www.ibm.com/	A-IBM-ASPE-060820/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			to buffer overflow after valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code through a service. IBM X-Force ID: 180902. **CVE ID : CVE-2020-4436**	support/pages/node/6221324	
aspera_shares_on_demand					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to command injection after valid authentication, which could allow an attacker with intimate knowledge of the system to execute commands in a SOAP API. IBM X-Force ID: 180810. **CVE ID : CVE-2020-4432**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/275
Out-of-bounds Write	10-06-2020	9.3	Certain IBM Aspera applications are vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker with intimate knowledge of the server to execute arbitrary code on the system with the privileges of root or cause server to crash. IBM X-Force ID: 180814. **CVE ID : CVE-2020-4433**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/276
Buffer Copy without Checking Size of Input ('Classic Buffer	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow based on the product configuration and valid authentication, which could allow an	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180900. **CVE ID : CVE-2020-4434**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-06-2020	6	Certain IBM Aspera applications are vulnerable to arbitrary memory corruption based on the product configuration, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180901. **CVE ID : CVE-2020-4435**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/278
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow after valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code through a service. IBM X-Force ID: 180902. **CVE ID : CVE-2020-4436**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/279
aspera_streaming					
Improper Neutralization of Special Elements in Output Used by a Downstream	10-06-2020	6	Certain IBM Aspera applications are vulnerable to command injection after valid authentication, which could allow an attacker with intimate knowledge of the system to execute	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			commands in a SOAP API. IBM X-Force ID: 180810. **CVE ID : CVE-2020-4432**		
Out-of-bounds Write	10-06-2020	9.3	Certain IBM Aspera applications are vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker with intimate knowledge of the server to execute arbitrary code on the system with the privileges of root or cause server to crash. IBM X-Force ID: 180814. **CVE ID : CVE-2020-4433**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/281
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow based on the product configuration and valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180900. **CVE ID : CVE-2020-4434**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/282
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-06-2020	6	Certain IBM Aspera applications are vulnerable to arbitrary memory corruption based on the product configuration, which could allow an attacker with intimate knowledge of the system to execute arbitrary	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180901. **CVE ID : CVE-2020-4435**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow after valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code through a service. IBM X-Force ID: 180902. **CVE ID : CVE-2020-4436**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/284
aspera_transfer_cluster_manager					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to command injection after valid authentication, which could allow an attacker with intimate knowledge of the system to execute commands in a SOAP API. IBM X-Force ID: 180810. **CVE ID : CVE-2020-4432**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/285
Out-of-bounds Write	10-06-2020	9.3	Certain IBM Aspera applications are vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker with intimate knowledge of the server to execute arbitrary code on the system with the privileges of root or cause server to crash. IBM X-Force ID: 180814.	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4433		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow based on the product configuration and valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180900. **CVE ID : CVE-2020-4434**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/287
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-06-2020	6	Certain IBM Aspera applications are vulnerable to arbitrary memory corruption based on the product configuration, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180901. **CVE ID : CVE-2020-4435**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/288
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-06-2020	6	Certain IBM Aspera applications are vulnerable to buffer overflow after valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code through a service. IBM X-Force ID: 180902. **CVE ID : CVE-2020-4436**	https://www.ibm.com/support/pages/node/6221324	A-IBM-ASPE-060820/289
api_connect					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2020	3.5	IBM API Connect 5.0.0.0 through 5.0.8.8 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 175489. **CVE ID : CVE-2020-4251**	https://www.ibm.com/support/pages/node/6209125	A-IBM-API_-060820/290
websphere_application_server					
Deserialization of Untrusted Data	05-06-2020	10	IBM WebSphere Application Server Network Deployment 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 181228. **CVE ID : CVE-2020-4448**	https://www.ibm.com/support/pages/node/6220336	A-IBM-WEBS-060820/291
Information Exposure	05-06-2020	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to obtain sensitive information with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181230. **CVE ID : CVE-2020-4449**	https://www.ibm.com/support/pages/node/6220296	A-IBM-WEBS-060820/292
Deserialization of Untrusted Data	05-06-2020	10	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system	https://www.ibm.com/support/pages/node/6220294	A-IBM-WEBS-060820/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181231. **CVE ID : CVE-2020-4450**		
websphere_virtual_enterprise					
Deserialization of Untrusted Data	05-06-2020	10	IBM WebSphere Application Server Network Deployment 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 181228. **CVE ID : CVE-2020-4448**	https://www.ibm.com/support/pages/node/6220336	A-IBM-WEBS-060820/294
maximo_asset_management					
Server-Side Request Forgery (SSRF)	08-06-2020	6.5	IBM Maximo Asset Management 7.6.0 and 7.6.1 is vulnerable to server side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 182713. **CVE ID : CVE-2020-4529**	https://www.ibm.com/support/pages/node/6220528	A-IBM-MAXI-060820/295
qradar_security_information_and_event_manager					
Improper Restriction of XML External Entity Reference	04-06-2020	5.5	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could	https://www.ibm.com/support/pages/node/6220154	A-IBM-QRAD-060820/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('XXE')			exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 182364. **CVE ID : CVE-2020-4509**		
Icinga					
icinga					
Improper Link Resolution Before File Access ('Link Following')	12-06-2020	4.6	An issue was discovered in Icinga2 before v2.12.0-rc1. The prepare-dirs script (run as part of the icinga2 systemd service) executes chmod 2750 /run/icinga2/cmd. /run/icinga2 is under control of an unprivileged user by default. If /run/icinga2/cmd is a symlink, then it will by followed and arbitrary files can be changed to mode 2750 by the unprivileged icinga2 user. **CVE ID : CVE-2020-14004**	http://www.openwall.com/lists/oss-security/2020/06/12/1	A-ICI-ICIN-060820/297
ijg					
libjpeg					
Uncontrolled Resource Consumption	15-06-2020	5.8	In IJG JPEG (aka libjpeg) before 9d, jpeg_mem_available() in jmemnobs.c in djpeg does not honor the max_memory_to_use setting, possibly causing excessive memory consumption. **CVE ID : CVE-2020-14152**	N/A	A-IJG-LIBJ-060820/298
Out-of-bounds Read	15-06-2020	5.8	In IJG JPEG (aka libjpeg) before 9d, jdhuff.c has an	N/A	A-IJG-LIBJ-060820/299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			out-of-bounds array read for certain table pointers. **CVE ID : CVE-2020-14153**		
ijinshan					
cheetah_free_wifi					
Improper Input Validation	05-06-2020	6.1	In Cheetah free WiFi 5.1, the driver file (liebaonat.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x830020f8, 0x830020E0, 0x830020E4, or 0x8300210c. **CVE ID : CVE-2020-13646**	N/A	A-IJI-CHEE-060820/300
Imagemagick					
imagemagick					
Out-of-bounds Read	07-06-2020	5.8	ImageMagick 7.0.9-27 through 7.0.10-17 has a heap-based buffer over-read in BlobToStringInfo in MagickCore/string.c during TIFF image decoding. **CVE ID : CVE-2020-13902**	N/A	A-IMA-IMAG-060820/301
Inductiveautomation					
ignition_gateway					
Deserialization of Untrusted Data	09-06-2020	5	The affected product lacks proper validation of user-supplied data, which can result in deserialization of untrusted data on the Ignition 8 Gateway (versions prior to 8.0.10) and Ignition 7 Gateway (versions prior to 7.9.14), allowing an attacker to obtain sensitive	N/A	A-IND-IGNI-060820/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information. **CVE ID : CVE-2020-10644**		
Deserialization of Untrusted Data	09-06-2020	5	The affected product is vulnerable to the handling of serialized data. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data on the Ignition 8 Gateway (versions prior to 8.0.10) and Ignition 7 Gateway (versions prior to 7.9.14), allowing an attacker to obtain sensitive information. **CVE ID : CVE-2020-12000**	N/A	A-IND-IGNI-060820/303
Missing Authentication for Critical Function	09-06-2020	5	The affected product lacks proper authentication required to query the server on the Ignition 8 Gateway (versions prior to 8.0.10) and Ignition 7 Gateway (versions prior to 7.9.14), allowing an attacker to obtain sensitive information. **CVE ID : CVE-2020-12004**	N/A	A-IND-IGNI-060820/304
Intel					
server_platform_services					
Improper Initialization	15-06-2020	4.6	Improper initialization in subsystem for Intel(R) SPS versions before SPS_E3_04.01.04.109.0 and SPS_E3_04.08.04.070.0 may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via	https://kc.mcafee.com/corporate/index?page=content&id=SB10321	A-INT-SERV-060820/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0586**		
Integer Overflow or Wraparound	15-06-2020	2.1	Integer overflow in subsystem for Intel(R) CSME versions before 11.8.77, 11.12.77, 11.22.77 and Intel(R) TXE versions before 3.1.75, 4.0.25 and Intel(R) Server Platform Services (SPS) versions before SPS_E5_04.01.04.380.0, SPS_SoC-X_04.00.04.128.0, SPS_SoC-A_04.00.04.211.0, SPS_E3_04.01.04.109.0, SPS_E3_04.08.04.070.0 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2020-0545**	https://cert-portal.siemens.com/productcert/pdf/ssa-631949.pdf, https://kc.mcafee.com/corporate/index?page=content&id=SB10321	A-INT-SERV-060820/306
active_management_technology					
Out-of-bounds Read	15-06-2020	5	Out-of-bounds read in IPv6 subsystem in Intel(R) AMT and Intel(R) ISM versions before 14.0.33 may allow an unauthenticated user to potentially enable denial of service via network access. **CVE ID : CVE-2020-0597**	https://www.synology.com/security/advisory/Synology_SA_20_15	A-INT-ACTI-060820/307
service_manager					
Out-of-bounds Read	15-06-2020	7.5	Out-of-bounds read in IPv6 subsystem in Intel(R) AMT and Intel(R) ISM versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	https://www.synology.com/security/advisory/Synology_SA_20_15	A-INT-SERV-060820/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0594		
Use After Free	15-06-2020	7.5	Use after free in IPv6 subsystem in Intel(R) AMT and Intel(R) ISM versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable escalation of privilege via network access. **CVE ID : CVE-2020-0595**	https://www.synology.com/security/advisory/Synology_SA_20_15	A-INT-SERV-060820/309
Improper Input Validation	15-06-2020	5	Improper input validation in DHCPv6 subsystem in Intel(R) AMT and Intel(R) ISM versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable information disclosure via network access. **CVE ID : CVE-2020-0596**	https://www.synology.com/security/advisory/Synology_SA_20_15	A-INT-SERV-060820/310
Out-of-bounds Read	15-06-2020	5	Out-of-bounds read in DHCPv6 subsystem in Intel(R) AMT and Intel(R)ISM versions before 11.8.77, 11.12.77, 11.22.77, 12.0.64 and 14.0.33 may allow an unauthenticated user to potentially enable information disclosure via network access. **CVE ID : CVE-2020-8674**	https://www.synology.com/security/advisory/Synology_SA_20_15	A-INT-SERV-060820/311
software_manager					
Out-of-bounds Read	15-06-2020	5	Out-of-bounds read in IPv6 subsystem in Intel(R) AMT and Intel(R) ISM versions before 14.0.33 may allow an unauthenticated user to	https://www.synology.com/security/advisory/Synology_S	A-INT-SOFT-060820/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via network access. **CVE ID : CVE-2020-0597**	A_20_15	
Irfanview					
irfanview					
N/A	10-06-2020	6.8	IrfanView 4.54 allows a user-mode write access violation starting at FORMATS!GetPlugInInfo+0x0000000000038ed4. **CVE ID : CVE-2020-13905**	N/A	A-IRF-IRFA-060820/313
N/A	10-06-2020	6.8	IrfanView 4.54 allows a user-mode write access violation starting at FORMATS!GetPlugInInfo+0x0000000000038eb7. **CVE ID : CVE-2020-13906**	N/A	A-IRF-IRFA-060820/314
istio					
istio					
NULL Pointer Dereference	02-06-2020	5	Istio 1.4.x before 1.4.9 and Istio 1.5.x before 1.5.4 contain the following vulnerability when telemetry v2 is enabled: by sending a specially crafted packet, an attacker could trigger a Null Pointer Exception resulting in a Denial of Service. This could be sent to the ingress gateway or a sidecar, triggering a null pointer exception which results in a denial of service. This also affects servicemesh-proxy where a null pointer exception flaw was found in servicemesh-proxy. When	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10739, https://istio.io/news/security/istio-security-2020-005/	A-IST-ISTI-060820/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			running Telemetry v2 (not on by default in version 1.4.x), an attacker could send a specially crafted packet to the ingress gateway or proxy sidecar, triggering a denial of service. **CVE ID : CVE-2020-10739**		
J2store					
j2store					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-06-2020	6.5	The J2Store plugin before 3.3.13 for Joomla! allows a SQL injection attack by a trusted store manager. **CVE ID : CVE-2020-13996**	N/A	A-J2S-J2ST-060820/316
Jenkins					
compact_columns					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	3.5	Jenkins Compact Columns Plugin 1.11 and earlier displays the unprocessed job description in tooltips, resulting in a stored cross-site scripting vulnerability that can be exploited by users with Job/Configure permission. **CVE ID : CVE-2020-2195**	https://jenkins.io/security/advisory/2020-06-03/#SECURITY-1837	A-JEN-COMP-060820/317
selenium					
Cross-Site Request Forgery (CSRF)	03-06-2020	6	Jenkins Selenium Plugin 3.141.59 and earlier has no CSRF protection for its HTTP endpoints, allowing attackers to perform all administrative actions	https://jenkins.io/security/advisory/2020-06-03/#SECURITY-1766	A-JEN-SELE-060820/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			provided by the plugin. **CVE ID : CVE-2020-2196**		
subversion_partial_release_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	4.3	Jenkins Subversion Partial Release Manager Plugin 1.0.1 and earlier does not escape the error message for the repository URL field form validation, resulting in a reflected cross-site scripting vulnerability. **CVE ID : CVE-2020-2199**	https://jenkins.io/security/advisory/2020-06-03/#SECURITY-1726	A-JEN-SUBV-060820/319
echarts_api					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	3.5	Jenkins ECharts API Plugin 4.7.0-3 and earlier does not escape the parser identifier when rendering charts, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2193**	https://jenkins.io/security/advisory/2020-06-03/#SECURITY-1841	A-JEN-ECHA-060820/320
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	3.5	Jenkins ECharts API Plugin 4.7.0-3 and earlier does not escape the display name of the builds in the trend chart, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2194**	https://jenkins.io/security/advisory/2020-06-03/#SECURITY-1842	A-JEN-ECHA-060820/321
play_framework					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	03-06-2020	6.5	Jenkins Play Framework Plugin 1.0.2 and earlier lets users specify the path to the `play` command on the Jenkins master for a form validation endpoint, resulting in an OS command injection vulnerability	https://jenkins.io/security/advisory/2020-06-03/#SECURITY-1879	A-JEN-PLAY-060820/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			exploitable by users able to store such a file on the Jenkins master. **CVE ID : CVE-2020-2200**		
project_inheritance					
Incorrect Default Permissions	03-06-2020	4	Jenkins Project Inheritance Plugin 19.08.02 and earlier does not require users to have Job/ExtendedRead permission to access Inheritance Project job configurations in XML format. **CVE ID : CVE-2020-2197**	https://jenkins.io/security/advisory/2020-06-03/#SECURITY-1582	A-JEN-PROJ-060820/323
Insufficiently Protected Credentials	03-06-2020	4	Jenkins Project Inheritance Plugin 19.08.02 and earlier does not redact encrypted secrets in the 'getConfigAsXML' API URL when transmitting job config.xml data to users without Job/Configure. **CVE ID : CVE-2020-2198**	https://jenkins.io/security/advisory/2020-06-03/#SECURITY-1582	A-JEN-PROJ-060820/324
script_security					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	3.5	Jenkins Script Security Plugin 1.72 and earlier does not correctly escape pending or approved classpath entries on the In-process Script Approval page, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2190**	https://jenkins.io/security/advisory/2020-06-03/#SECURITY-1866	A-JEN-SCRI-060820/325
self-organizing_swarm_modules					
Incorrect Default Permissions	03-06-2020	4	Jenkins Self-Organizing Swarm Plug-in Modules Plugin 3.20 and earlier does not check permissions on	https://jenkins.io/security/advisory/2020-06-	A-JEN-SELF-060820/326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			API endpoints that allow adding and removing agent labels. **CVE ID : CVE-2020-2191**	03/#SECURITY-1200	
Cross-Site Request Forgery (CSRF)	03-06-2020	4.3	A cross-site request forgery vulnerability in Jenkins Self-Organizing Swarm Plug-in Modules Plugin 3.20 and earlier allows attackers to add or remove agent labels. **CVE ID : CVE-2020-2192**	https://jenkins.io/security/advisory/2020-06-03/#SECURITY-1200	A-JEN-SELF-060820/327
Jerryscript					
jerryscript					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	5	An issue was discovered in ecma/operations/ecma-container-object.c in JerryScript 2.2.0. Operations with key/value pairs did not consider the case where garbage collection is triggered after the key operation but before the value operation, as demonstrated by improper read access to memory in ecma_gc_set_object_visited in ecma/base/ecma-gc.c. **CVE ID : CVE-2020-14163**	N/A	A-JER-JERR-060820/328
Joomla					
joomla\!					
Cross-Site Request Forgery (CSRF)	02-06-2020	6.8	In Joomla! before 3.9.19, missing token checks in com_postinstall lead to CSRF. **CVE ID : CVE-2020-13760**	N/A	A-JOO-JOOM-060820/329
Improper Neutralization of Input	02-06-2020	4.3	In Joomla! before 3.9.19, lack of input validation in the heading tag option of the	N/A	A-JOO-JOOM-060820/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			"Articles - Newsflash" and "Articles - Categories" modules allows XSS. **CVE ID : CVE-2020-13761**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-06-2020	4.3	In Joomla! before 3.9.19, incorrect input validation of the module tag option in com_modules allows XSS. **CVE ID : CVE-2020-13762**	N/A	A-JOO-JOOM-060820/331
Improper Preservation of Permissions	02-06-2020	5	In Joomla! before 3.9.19, the default settings of the global textfilter configuration do not block HTML inputs for Guest users. **CVE ID : CVE-2020-13763**	N/A	A-JOO-JOOM-060820/332
katacontainers					
runtime					
Improper Privilege Management	10-06-2020	4.6	Kata Containers doesn't restrict containers from accessing the guest's root filesystem device. Malicious containers can exploit this to gain code execution on the guest and masquerade as the kata-agent. This issue affects Kata Containers 1.11 versions earlier than 1.11.1; Kata Containers 1.10 versions earlier than 1.10.5; and Kata Containers 1.9 and earlier versions. **CVE ID : CVE-2020-2023**	N/A	A-KAT-RUNT-060820/333
Improper Link Resolution	10-06-2020	4.6	A malicious guest compromised before a container creation (e.g. a	N/A	A-KAT-RUNT-060820/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Before File Access ('Link Following')			malicious guest image or a guest running multiple containers) can trick the kata runtime into mounting the untrusted container filesystem on any host path, potentially allowing for code execution on the host. This issue affects: Kata Containers 1.11 versions earlier than 1.11.1; Kata Containers 1.10 versions earlier than 1.10.5; Kata Containers 1.9 and earlier versions. **CVE ID : CVE-2020-2026**		
Kubernetes					
kubernetes					
Server-Side Request Forgery (SSRF)	05-06-2020	3.5	The Kubernetes kube-controller-manager in versions v1.0-1.14, versions prior to v1.15.12, v1.16.9, v1.17.5, and version v1.18.0 are vulnerable to a Server Side Request Forgery (SSRF) that allows certain authorized users to leak up to 500 bytes of arbitrary information from unprotected endpoints within the master's host network (such as link-local or loopback services). **CVE ID : CVE-2020-8555**	https://github.com/kubernetes/kubernetes/issues/91542	A-KUB-KUBE-060820/335
kumbiaphp					
kumbiaphp					
Improper Neutralization of Input	15-06-2020	3.5	KumbiaPHP through 1.1.1, in Development mode, allows XSS via the	N/A	A-KUM-KUMB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			public/pages/kumbia PATH_INFO. **CVE ID : CVE-2020-14146**		060820/336
laborator					
neon					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-06-2020	3.5	The Neon theme 2.0 before 2020-06-03 for Bootstrap allows XSS via an Add Task Input operation in a dashboard. **CVE ID : CVE-2020-13890**	N/A	A-LAB-NEON-060820/337
xenon					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-06-2020	4.3	The Laborator Xenon theme 1.3 for WordPress allows Reflected XSS via the data/typeahead-generate.php q (aka name) parameter. **CVE ID : CVE-2020-14010**	N/A	A-LAB-XENO-060820/338
Lansweeper					
lansweeper					
Incorrect Authorization	15-06-2020	7.5	Lansweeper 6.0.x through 7.2.x has a default installation in which the admin password is configured for the admin account, unless "Built-in admin" is manually unchecked. This allows command execution via the Add New Package and Scheduled Deployments features.	N/A	A-LAN-LANS-060820/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14011		
libemf_project					
libemf					
Integer Overflow or Wraparound	15-06-2020	4.3	ScaleViewPortExtEx in libemf.cpp in libEMF (aka ECMA-234 Metafile Library) 1.0.12 allows an integer overflow and denial of service via a crafted EMF file. **CVE ID : CVE-2020-13999**	N/A	A-LIB-LIBE-060820/340
libjpeg-turbo					
libjpeg-turbo					
Out-of-bounds Read	03-06-2020	5.8	libjpeg-turbo 2.0.4, and mozjpeg 4.0.0, has a heap-based buffer over-read in get_rgb_row() in rdppm.c via a malformed PPM input file. **CVE ID : CVE-2020-13790**	N/A	A-LIB-LIBJ-060820/341
Libreoffice					
libreoffice					
Information Exposure	08-06-2020	4.3	LibreOffice has a 'stealth mode' in which only documents from locations deemed 'trusted' are allowed to retrieve remote resources. This mode is not the default mode, but can be enabled by users who want to disable LibreOffice's ability to include remote resources within a document. A flaw existed where remote graphic links loaded from docx documents were omitted from this protection prior to version 6.4.4. This issue affects: The Document Foundation LibreOffice	N/A	A-LIB-LIBR-060820/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 6.4.4. **CVE ID : CVE-2020-12802**		
Improper Input Validation	08-06-2020	4.3	ODF documents can contain forms to be filled out by the user. Similar to HTML forms, the contained form data can be submitted to a URI, for example, to an external web server. To create submittable forms, ODF implements the XForms W3C standard, which allows data to be submitted without the need for macros or other active scripting Prior to version 6.4.4 LibreOffice allowed forms to be submitted to any URI, including file: URIs, enabling form submissions to overwrite local files. User-interaction is required to submit the form, but to avoid the possibility of malicious documents engineered to maximize the possibility of inadvertent user submission this feature has now been limited to http[s] URIs, removing the possibility to overwrite local files. This issue affects: The Document Foundation LibreOffice versions prior to 6.4.4. **CVE ID : CVE-2020-12803**	N/A	A-LIB-LIBR-060820/343
libupnp_project					
libupnp					
NULL Pointer	04-06-2020	5	Portable UPnP SDK (aka libupnp) 1.12.1 and earlier	N/A	A-LIB-LIBU-060820/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			allows remote attackers to cause a denial of service (crash) via a crafted SSDP message due to a NULL pointer dereference in the functions FindServiceControlURLPath and FindServiceEventURLPath in genlib/service_table/service_table.c. **CVE ID : CVE-2020-13848**		
Liferay					
liferay_portal					
N/A	10-06-2020	4	Liferay Portal 7.x before 7.3.2, and Liferay DXP 7.0 before fix pack 92, 7.1 before fix pack 18, and 7.2 before fix pack 5 does not sanitize the information returned by the DDMDataProvider API, which allows remote authenticated users to obtain the password to REST Data Providers. **CVE ID : CVE-2020-13444**	https://issues.liferay.com/browse/LPE-17009, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/119317396	A-LIF-LIFE-060820/345
N/A	10-06-2020	6.5	In Liferay Portal before 7.3.2 and Liferay DXP 7.0 before fix pack 92, 7.1 before fix pack 18, and 7.2 before fix pack 6, the template API does not restrict user access to sensitive objects, which allows remote authenticated users to execute arbitrary	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5	A-LIF-LIFE-060820/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code via crafted FreeMarker and Velocity templates. **CVE ID : CVE-2020-13445**	mxmVrnXW/content/id/119317411	
Linuxfoundation					
indy-node					
Uncontrolled Resource Consumption	11-06-2020	5	In Indy Node 1.12.2, there is an Uncontrolled Resource Consumption vulnerability. Indy Node has a bug in TAA handling code. The current primary can be crashed with a malformed transaction from a client, which leads to a view change. Repeated rapid view changes have the potential of bringing down the network. This is fixed in version 1.12.3. **CVE ID : CVE-2020-11090**	https://github.com/hyperledger/indy-node/security/advisories/GHSA-3gw4-m5w7-v89c	A-LIN-INDY-060820/347
linuxtv					
xawtv					
Incorrect Permission Assignment for Critical Resource	08-06-2020	3.6	An issue was discovered in LinuxTV xawtv before 3.107. The function dev_open() in v4l-conf.c does not perform sufficient checks to prevent an unprivileged caller of the program from opening unintended filesystem paths. This allows a local attacker with access to the v4l-conf setuid-root program to test for the existence of arbitrary files and to trigger an open on arbitrary files with mode O_RDWR. To achieve this, relative path components need to be added to the	http://www.openwall.com/lists/oss-security/2020/06/04/6	A-LIN-XAWT-060820/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device path, as demonstrated by a v4l-conf -c /dev/../root/.bash_history command. **CVE ID : CVE-2020-13696**		
Mcafee					
host_intrusion_prevention					
Untrusted Search Path	10-06-2020	4.4	DLL Search Order Hijacking Vulnerability in the installer component of McAfee Host Intrusion Prevention System (Host IPS) for Windows prior to 8.0.0 Patch 15 Update allows attackers with local access to execute arbitrary code via execution from a compromised folder. **CVE ID : CVE-2020-7279**	https://kc.mcafee.com/corporate/index?page=content&id=SB10320	A-MCA-HOST-060820/349
virusscan_enterprise					
Improper Privilege Management	10-06-2020	4.6	Privilege Escalation vulnerability during daily DAT updates when using McAfee Virus Scan Enterprise (VSE) prior to 8.8 Patch 15 allows local users to cause the deletion and creation of files they would not normally have permission to through altering the target of symbolic links. This is timing dependent. **CVE ID : CVE-2020-7280**	https://kc.mcafee.com/corporate/index?page=content&id=SB10302	A-MCA-VIRU-060820/350
Mediawiki					
mediawiki					
URL Redirection to Untrusted	02-06-2020	5.8	resources/src/mediawiki.page.ready/ready.js in MediaWiki before 1.35	N/A	A-MED-MEDI-060820/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			allows remote attackers to force a logout and external redirection via HTML content in a MediaWiki page. **CVE ID : CVE-2020-10959**		
meetecho					
janus					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-06-2020	7.5	An issue was discovered in janus-gateway (aka Janus WebRTC Server) through 0.10.0. janus_streaming_rtsp_parse_sdp in plugins/janus_streaming.c has a Buffer Overflow via a crafted RTSP server. **CVE ID : CVE-2020-14033**	https://github.com/meetecho/janus-gateway/pull/2229	A-MEE-JANU-060820/352
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-06-2020	7.5	An issue was discovered in janus-gateway (aka Janus WebRTC Server) through 0.10.0. janus_get_codec_from_pt in utils.c has a Buffer Overflow via long value in an SDP Offer packet. **CVE ID : CVE-2020-14034**	https://github.com/meetecho/janus-gateway/pull/2229	A-MEE-JANU-060820/353
NULL Pointer Dereference	10-06-2020	5	An issue was discovered in janus-gateway (aka Janus WebRTC Server) through 0.10.0. janus_sdp_process in sdp.c has a NULL pointer dereference. **CVE ID : CVE-2020-13898**	https://github.com/meetecho/janus-gateway/pull/2214	A-MEE-JANU-060820/354
Missing Initialization of Resource	10-06-2020	5	An issue was discovered in janus-gateway (aka Janus WebRTC Server) through 0.10.0. janus_process_incoming_req	https://github.com/meetecho/janus-gateway/pu	A-MEE-JANU-060820/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			uest in janus.c discloses information from uninitialized stack memory. **CVE ID : CVE-2020-13899**	ll/2214	
NULL Pointer Dereference	10-06-2020	5	An issue was discovered in janus-gateway (aka Janus WebRTC Server) through 0.10.0. janus_sdp_preparse in sdp.c has a NULL pointer dereference. **CVE ID : CVE-2020-13900**	https://github.com/meetecho/janus-gateway/pull/2214	A-MEE-JANU-060820/356
Out-of-bounds Write	10-06-2020	7.5	An issue was discovered in janus-gateway (aka Janus WebRTC Server) through 0.10.0. janus_sdp_merge in sdp.c has a stack-based buffer overflow. **CVE ID : CVE-2020-13901**	https://github.com/meetecho/janus-gateway/pull/2214	A-MEE-JANU-060820/357
Microfocus					
arcsight_logger					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2020	4.3	Cross Site Scripting (XSS) vulnerability in Micro Focus ArcSight Logger product, affecting all version from 6.6.1 up to version 7.0.1. The vulnerabilities could be remotely exploited resulting in Cross-Site Scripting (XSS) or information disclosure. **CVE ID : CVE-2020-11839**	N/A	A-MIC-ARCS-060820/358
Microsoft					
365_apps					
Improper Restriction of Operations within the	09-06-2020	6.8	A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory,	N/A	A-MIC-365_-060820/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			aka 'Microsoft Office Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1321**		
Information Exposure	09-06-2020	4.3	An information disclosure vulnerability exists when Microsoft Project reads out of bound memory due to an uninitialized variable, aka 'Microsoft Project Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1322**	N/A	A-MIC-365_-060820/360
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1226. **CVE ID : CVE-2020-1225**	N/A	A-MIC-365_-060820/361
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1225. **CVE ID : CVE-2020-1226**	N/A	A-MIC-365_-060820/362
Information Exposure	09-06-2020	4.3	A security feature bypass vulnerability exists in Microsoft Outlook when Office fails to enforce	N/A	A-MIC-365_-060820/363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security settings configured on a system, aka 'Microsoft Outlook Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1229**		
windows_defender					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170. **CVE ID : CVE-2020-1163**	N/A	A-MIC-WIND-060820/364
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163. **CVE ID : CVE-2020-1170**	N/A	A-MIC-WIND-060820/365
forefront_endpoint_protection_2010					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion	N/A	A-MIC-FORE-060820/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170. **CVE ID : CVE-2020-1163**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163. **CVE ID : CVE-2020-1170**	N/A	A-MIC-FORE-060820/367
system_center_endpoint_protection					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170. **CVE ID : CVE-2020-1163**	N/A	A-MIC-SYST-060820/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163. **CVE ID : CVE-2020-1170**	N/A	A-MIC-SYST-060820/369
security_essentials					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170. **CVE ID : CVE-2020-1163**	N/A	A-MIC-SECU-060820/370
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is	N/A	A-MIC-SECU-060820/371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2020-1163. **CVE ID : CVE-2020-1170**		
project					
Information Exposure	09-06-2020	4.3	An information disclosure vulnerability exists when Microsoft Project reads out of bound memory due to an uninitialized variable, aka 'Microsoft Project Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1322**	N/A	A-MIC-PROJ-060820/372
bing					
Authentication Bypass by Spoofing	09-06-2020	4.3	A spoofing vulnerability exists when Microsoft Bing Search for Android improperly handles specific HTML content, aka 'Microsoft Bing Search Spoofing Vulnerability'. **CVE ID : CVE-2020-1329**	N/A	A-MIC-BING-060820/373
system_center_operations_manager					
Authentication Bypass by Spoofing	09-06-2020	3.5	A spoofing vulnerability exists when System Center Operations Manager (SCOM) does not properly sanitize a specially crafted web request to an affected SCOM instance, aka 'System Center Operations Manager Spoofing Vulnerability'. **CVE ID : CVE-2020-1331**	N/A	A-MIC-SYST-060820/374
nugetgallery					
Improper Neutralization of Input	09-06-2020	3.5	A spoofing vulnerability exists when the NuGetGallery does not	N/A	A-MIC-NUGE-060820/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			properly sanitize input on package metadata values, aka 'NuGetGallery Spoofing Vulnerability'. **CVE ID : CVE-2020-1340**		
visual_studio					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1203. **CVE ID : CVE-2020-1202**	N/A	A-MIC-VISU-060820/376
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1202. **CVE ID : CVE-2020-1203**	N/A	A-MIC-VISU-060820/377
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of	N/A	A-MIC-VISU-060820/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1278, CVE-2020-1293. **CVE ID : CVE-2020-1257**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1293. **CVE ID : CVE-2020-1278**	N/A	A-MIC-VISU-060820/379
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1278. **CVE ID : CVE-2020-1293**	N/A	A-MIC-VISU-060820/380
chakracore					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1073**	N/A	A-MIC-CHAK-060820/381
Improper Restriction of	09-06-2020	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers	N/A	A-MIC-CHAK-060820/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1219**		
edge					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1073**	N/A	A-MIC-EDGE-060820/383
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1219**	N/A	A-MIC-EDGE-060820/384
URL Redirection to Untrusted Site ('Open Redirect')	09-06-2020	5.8	A spoofing vulnerability exists when theMicrosoft Edge (Chromium-based) in IE Mode improperly handles specific redirects, aka 'Microsoft Edge (Chromium-based) in IE Mode Spoofing Vulnerability'. **CVE ID : CVE-2020-1220**	N/A	A-MIC-EDGE-060820/385
Information Exposure	09-06-2020	2.6	An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests, aka 'Microsoft Edge Information Disclosure Vulnerability'.	N/A	A-MIC-EDGE-060820/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1242		
office					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory, aka 'Microsoft Office Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1321**	N/A	A-MIC-OFFI-060820/387
Information Exposure	09-06-2020	4.3	An information disclosure vulnerability exists when Microsoft Project reads out of bound memory due to an uninitialized variable, aka 'Microsoft Project Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1322**	N/A	A-MIC-OFFI-060820/388
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1226. **CVE ID : CVE-2020-1225**	N/A	A-MIC-OFFI-060820/389
Improper Restriction of Operations within the Bounds of a Memory	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'.	N/A	A-MIC-OFFI-060820/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			This CVE ID is unique from CVE-2020-1225. **CVE ID : CVE-2020-1226**		
Information Exposure	09-06-2020	4.3	A security feature bypass vulnerability exists in Microsoft Outlook when Office fails to enforce security settings configured on a system, aka 'Microsoft Outlook Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1229**	N/A	A-MIC-OFFI-060820/391
internet_explorer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1213**	N/A	A-MIC-INTE-060820/392
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1214**	N/A	A-MIC-INTE-060820/393
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine	N/A	A-MIC-INTE-060820/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1215**		
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1216**	N/A	A-MIC-INTE-060820/395
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1219**	N/A	A-MIC-INTE-060820/396
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1260. **CVE ID : CVE-2020-1230**	N/A	A-MIC-INTE-060820/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230. **CVE ID : CVE-2020-1260**	N/A	A-MIC-INTE-060820/398
Information Exposure	09-06-2020	2.6	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory, aka 'Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1315**	N/A	A-MIC-INTE-060820/399
visual_studio_2017					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1203. **CVE ID : CVE-2020-1202**	N/A	A-MIC-VISU-060820/400
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in	N/A	A-MIC-VISU-060820/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1202. **CVE ID : CVE-2020-1203**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1278, CVE-2020-1293. **CVE ID : CVE-2020-1257**	N/A	A-MIC-VISU-060820/402
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1293. **CVE ID : CVE-2020-1278**	N/A	A-MIC-VISU-060820/403
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1278.	N/A	A-MIC-VISU-060820/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1293		
sharepoint_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1183, CVE-2020-1297, CVE-2020-1298, CVE-2020-1318, CVE-2020-1320. **CVE ID : CVE-2020-1177**	N/A	A-MIC-SHAR-060820/405
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1183, CVE-2020-1297, CVE-2020-1298, CVE-2020-1320. **CVE ID : CVE-2020-1318**	N/A	A-MIC-SHAR-060820/406
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE	N/A	A-MIC-SHAR-060820/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID is unique from CVE-2020-1177, CVE-2020-1183, CVE-2020-1297, CVE-2020-1298, CVE-2020-1318. **CVE ID : CVE-2020-1320**		
URL Redirection to Untrusted Site ('Open Redirect')	09-06-2020	5.8	An open redirect vulnerability exists in Microsoft SharePoint that could lead to spoofing.To exploit the vulnerability, an attacker could send a link that has a specially crafted URL and convince the user to click the link, aka 'SharePoint Open Redirect Vulnerability'. **CVE ID : CVE-2020-1323**	N/A	A-MIC-SHAR-060820/408
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1289. **CVE ID : CVE-2020-1148**	N/A	A-MIC-SHAR-060820/409
Improper Privilege Management	09-06-2020	6.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted authentication request to an affected SharePoint server, aka 'Microsoft SharePoint Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1178**	N/A	A-MIC-SHAR-060820/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-06-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls, aka 'Microsoft SharePoint Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1181**	N/A	A-MIC-SHAR-060820/411
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1297, CVE-2020-1298, CVE-2020-1318, CVE-2020-1320. **CVE ID : CVE-2020-1183**	N/A	A-MIC-SHAR-060820/412
Improper Privilege Management	09-06-2020	6.5	An elevation of privilege vulnerability exists in Microsoft SharePoint, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1295**	N/A	A-MIC-SHAR-060820/413
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint	N/A	A-MIC-SHAR-060820/414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1183, CVE-2020-1298, CVE-2020-1318, CVE-2020-1320. **CVE ID : CVE-2020-1297**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1183, CVE-2020-1297, CVE-2020-1318, CVE-2020-1320. **CVE ID : CVE-2020-1298**	N/A	A-MIC-SHAR-060820/415
word					
Improper Input Validation	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Word for Android fails to properly handle certain files.To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted URL file.The update addresses the vulnerability by correcting how Microsoft Word for Android handles specially crafted URL files., aka 'Word for Android Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1223**	N/A	A-MIC-WORD-060820/416
Information	09-06-2020	4.3	A security feature bypass	N/A	A-MIC-WORD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			vulnerability exists in Microsoft Outlook when Office fails to enforce security settings configured on a system, aka 'Microsoft Outlook Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1229**		060820/417
sharepoint_enterprise_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1183, CVE-2020-1297, CVE-2020-1298, CVE-2020-1318, CVE-2020-1320. **CVE ID : CVE-2020-1177**	N/A	A-MIC-SHAR-060820/418
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1183, CVE-2020-1297, CVE-2020-1298, CVE-2020-1320. **CVE ID : CVE-2020-1318**	N/A	A-MIC-SHAR-060820/419
Improper Neutralizatio	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when	N/A	A-MIC-SHAR-060820/420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1183, CVE-2020-1297, CVE-2020-1298, CVE-2020-1318. **CVE ID : CVE-2020-1320**		
URL Redirection to Untrusted Site ('Open Redirect')	09-06-2020	5.8	An open redirect vulnerability exists in Microsoft SharePoint that could lead to spoofing.To exploit the vulnerability, an attacker could send a link that has a specially crafted URL and convince the user to click the link, aka 'SharePoint Open Redirect Vulnerability'. **CVE ID : CVE-2020-1323**	N/A	A-MIC-SHAR-060820/421
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1289. **CVE ID : CVE-2020-1148**	N/A	A-MIC-SHAR-060820/422
Improper Privilege Management	09-06-2020	6.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a	N/A	A-MIC-SHAR-060820/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted authentication request to an affected SharePoint server, aka 'Microsoft SharePoint Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1178**		
Improper Input Validation	09-06-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls, aka 'Microsoft SharePoint Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1181**	N/A	A-MIC-SHAR-060820/424
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1297, CVE-2020-1298, CVE-2020-1318, CVE-2020-1320. **CVE ID : CVE-2020-1183**	N/A	A-MIC-SHAR-060820/425
Improper Privilege Management	09-06-2020	6.5	An elevation of privilege vulnerability exists in Microsoft SharePoint, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1295**	N/A	A-MIC-SHAR-060820/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1183, CVE-2020-1298, CVE-2020-1318, CVE-2020-1320. **CVE ID : CVE-2020-1297**	N/A	A-MIC-SHAR-060820/427
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1183, CVE-2020-1297, CVE-2020-1318, CVE-2020-1320. **CVE ID : CVE-2020-1298**	N/A	A-MIC-SHAR-060820/428
sharepoint_foundation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1183, CVE-2020-1297, CVE-	N/A	A-MIC-SHAR-060820/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1298, CVE-2020-1318, CVE-2020-1320. **CVE ID : CVE-2020-1177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1183, CVE-2020-1297, CVE-2020-1298, CVE-2020-1320. **CVE ID : CVE-2020-1318**	N/A	A-MIC-SHAR-060820/430
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1183, CVE-2020-1297, CVE-2020-1298, CVE-2020-1318. **CVE ID : CVE-2020-1320**	N/A	A-MIC-SHAR-060820/431
Improper Input Validation	09-06-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls, aka 'Microsoft SharePoint Server Remote Code Execution	N/A	A-MIC-SHAR-060820/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1297, CVE-2020-1298, CVE-2020-1318, CVE-2020-1320. **CVE ID : CVE-2020-1183**	N/A	A-MIC-SHAR-060820/433
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1148. **CVE ID : CVE-2020-1289**	N/A	A-MIC-SHAR-060820/434
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1183, CVE-2020-1298, CVE-2020-1318,	N/A	A-MIC-SHAR-060820/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1320. **CVE ID : CVE-2020-1297**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1177, CVE-2020-1183, CVE-2020-1297, CVE-2020-1318, CVE-2020-1320. **CVE ID : CVE-2020-1298**	N/A	A-MIC-SHAR-060820/436
excel					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1226. **CVE ID : CVE-2020-1225**	N/A	A-MIC-EXCE-060820/437
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1225.	N/A	A-MIC-EXCE-060820/438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1226		
visual_studio_2019					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1203. **CVE ID : CVE-2020-1202**	N/A	A-MIC-VISU-060820/439
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1202. **CVE ID : CVE-2020-1203**	N/A	A-MIC-VISU-060820/440
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1278, CVE-2020-1293. **CVE ID : CVE-2020-1257**	N/A	A-MIC-VISU-060820/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1293. **CVE ID : CVE-2020-1278**	N/A	A-MIC-VISU-060820/442
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1278. **CVE ID : CVE-2020-1293**	N/A	A-MIC-VISU-060820/443
visual_studio_live_share					
Information Exposure	09-06-2020	5	An information disclosure vulnerability exists in Visual Studio Code Live Share Extension when it exposes tokens in plain text, aka 'Visual Studio Code Live Share Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1343**	N/A	A-MIC-VISU-060820/444
mids_reborn_hero_designer_project					
mids_reborn_hero_designer					
Uncontrolled Search Path Element	11-06-2020	4.4	Mids' Reborn Hero Designer 2.6.0.7 has an elevation of privilege vulnerability due to default and insecure	N/A	A-MID-MIDS-060820/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permissions being set for the installation folder. By default, the Authenticated Users group has Modify permissions to the installation folder. Because of this, any user on the system can replace binaries or plant malicious DLLs to obtain elevated, or different, privileges, depending on the context of the user that runs the application. **CVE ID : CVE-2020-11613**		
Cleartext Transmission of Sensitive Information	11-06-2020	6.8	Mids' Reborn Hero Designer 2.6.0.7 downloads the update manifest, as well as update files, over cleartext HTTP. Additionally, the application does not perform file integrity validation for files after download. An attacker can perform a man-in-the-middle attack against this connection and replace executable files with malicious versions, which the operating system then executes under the context of the user running Hero Designer. **CVE ID : CVE-2020-11614**	N/A	A-MID-MIDS-060820/446
minishare_project					
minishare					
Out-of-bounds Write	04-06-2020	7.5	In MiniShare before 1.4.2, there is a stack-based buffer overflow via an HTTP PUT request, which allows an attacker to achieve arbitrary	N/A	A-MIN-MINI-060820/447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution, a similar issue to CVE-2018-19861, CVE-2018-19862, and CVE-2019-17601. NOTE: this product is discontinued. **CVE ID : CVE-2020-13768**		
Mitel					
micollab_audio\,_web_\&_video_conferencing					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-06-2020	5	A Directory Traversal vulnerability in the web conference component of Mitel MiCollab AWV before 8.1.2.4 and 9.x before 9.1.3 could allow an attacker to access arbitrary files from restricted directories of the server via a crafted URL, due to insufficient access validation. A successful exploit could allow an attacker to access sensitive information from the restricted directories. **CVE ID : CVE-2020-11798**	https://www.mitel.com/-/media/mitel/file/pdf/support/security-advisories/security-bulletin-20-0005-01.pdf, https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-20-0005	A-MIT-MICO-060820/448
Monstra					
monstra_cms					
Improper Neutralization of Special Elements used in an OS Command ('OS	09-06-2020	6.5	** DISPUTED ** Monstra CMS 3.0.4 allows an attacker, who already has administrative access to modify .chunk.php files on the Edit Chunk screen, to execute arbitrary OS	N/A	A-MON-MONS-060820/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			commands via the Theme Module by visiting the admin/index.php?id=themes &action=edit_chunk URI. NOTE: there is no indication that the Edit Chunk feature was intended to prevent an administrator from using PHP's exec feature. **CVE ID : CVE-2020-13978**		
morganstanley					
hobbes					
Out-of-bounds Write	12-06-2020	7.5	In Morgan Stanley Hobbes through 2020-05-21, the array implementation lacks bounds checking, allowing exploitation of an out-of-bounds (OOB) read/write vulnerability that leads to both local and remote code (via RPC) execution. **CVE ID : CVE-2020-13656**	N/A	A-MOR-HOBB-060820/450
mosc_project					
mosc					
Improper Input Validation	10-06-2020	7.5	mosc through 1.0.0 is vulnerable to Arbitrary Code Execution. User input provided to `properties` argument is executed by the `eval` function, resulting in code execution. **CVE ID : CVE-2020-7672**	N/A	A-MOS-MOSC-060820/451
Mozilla					
mozjpeg					
Out-of-bounds Read	03-06-2020	5.8	libjpeg-turbo 2.0.4, and mozjpeg 4.0.0, has a heap-based buffer over-read in	N/A	A-MOZ-MOZJ-060820/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			get_rgb_row() in rdppm.c via a malformed PPM input file. **CVE ID : CVE-2020-13790**		
mqtt					
mqtt					
Uncontrolled Resource Consumption	04-06-2020	5	The MQTT protocol 3.1.1 requires a server to set a timeout value of 1.5 times the Keep-Alive value specified by a client, which allows remote attackers to cause a denial of service (loss of the ability to establish new connections), as demonstrated by SlowITe. **CVE ID : CVE-2020-13849**	N/A	A-MQT-MQTT-060820/453
Mumble					
mumble					
N/A	09-06-2020	5	Qt 5.12.2 through 5.14.2, as used in unofficial builds of Mumble 1.3.0 and other products, mishandles OpenSSL's error queue, which can cause a denial of service to QSslSocket users. Because errors leak in unrelated TLS sessions, an unrelated session may be disconnected when any handshake fails. (Mumble 1.3.1 is not affected, regardless of the Qt version.) **CVE ID : CVE-2020-13962**	N/A	A-MUM-MUMB-060820/454
Mutt					
mutt					
N/A	15-06-2020	5.8	Mutt before 1.14.3 proceeds with a connection even if, in	N/A	A-MUT-MUTT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			response to a GnuTLS certificate prompt, the user rejects an expired intermediate certificate. **CVE ID : CVE-2020-14154**		060820/455
Information Exposure	15-06-2020	4.3	Mutt before 1.14.3 allows an IMAP fcc/postpone man-in-the-middle attack via a PREAUTH response. **CVE ID : CVE-2020-14093**	N/A	A-MUT-MUTT-060820/456
Nagios					
nagios					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-06-2020	4	Nagios 4.4.5 allows an attacker, who already has administrative access to change the "URL for JSON CGIs" configuration setting, to modify the Alert Histogram and Trends code via crafted versions of the archivejson.cgi, objectjson.cgi, and statusjson.cgi files. NOTE: this vulnerability has been mistakenly associated with CVE-2020-1408. **CVE ID : CVE-2020-13977**	N/A	A-NAG-NAGI-060820/457
naviwebs					
navigatecms					
Unrestricted Upload of File with Dangerous Type	15-06-2020	7.5	The install_from_hash functionality in Navigate CMS 2.9 does not consider the .phtml extension when examining files within a ZIP archive that may contain PHP code, in check_upload in lib/packages/extensions/extension.class.php and	N/A	A-NAV-NAVI-060820/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lib/packages/themes/theme.class.php. **CVE ID : CVE-2020-14067**		
navigate_cms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-06-2020	5	An issue was discovered in Navigate CMS through 2.8.7. It allows Directory Traversal because lib/packages/templates/template.class.php mishandles ../ and ..\ substrings. **CVE ID : CVE-2020-13795**	N/A	A-NAV-NAVI-060820/459
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	4.3	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/structure/structure.class.php. **CVE ID : CVE-2020-13796**	N/A	A-NAV-NAVI-060820/460
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	4.3	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/websites/website.class.php. **CVE ID : CVE-2020-13797**	N/A	A-NAV-NAVI-060820/461
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2020	4.3	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/feeds/feed.class.php. **CVE ID : CVE-2020-13798**	N/A	A-NAV-NAVI-060820/462
Netapp					
solidfire_\&_hci_management_node					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	03-06-2020	6.2	systemd through v245 mishandles numerical usernames such as ones composed of decimal digits or 0x followed by hex digits, as demonstrated by use of root privileges when privileges of the 0x0 user account were intended. NOTE: this issue exists because of an incomplete fix for CVE-2017-1000082. **CVE ID : CVE-2020-13776**	https://security.netapp.com/advisory/ntap-20200611-0003/	A-NET-SOLI-060820/463
clustered_data_ontap					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.2	In FreeBSD 12.1-STABLE before r361918, 12.1-RELEASE before p6, 11.4-STABLE before r361919, 11.3-RELEASE before p10, and 11.4-RC2 before p1, an invalid memory location may be used for HID items if the push/pop level is not restored within the processing of that HID item allowing an attacker with physical access to a USB port to be able to use a specially crafted USB device to gain kernel or user-space code execution. **CVE ID : CVE-2020-7456**	https://security.netapp.com/advisory/ntap-20200625-0005/	A-NET-CLUS-060820/464
active_iq_unified_manager					
Improper Input Validation	03-06-2020	6.2	systemd through v245 mishandles numerical usernames such as ones composed of decimal digits or 0x followed by hex digits, as demonstrated by use of	https://security.netapp.com/advisory/ntap-20200611-0003/	A-NET-ACTI-060820/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			root privileges when privileges of the 0x0 user account were intended. NOTE: this issue exists because of an incomplete fix for CVE-2017-1000082. **CVE ID : CVE-2020-13776**		
Nextcloud					
talk					
Improper Control of Generation of Code ('Code Injection')	08-06-2020	6.5	A too lax check in Nextcloud Talk 6.0.4, 7.0.2 and 8.0.7 allowed a code injection when a not correctly sanitized talk command was added by an administrator. **CVE ID : CVE-2020-8180**	N/A	A-NEX-TALK-060820/466
Nghttp2					
nghttp2					
Improper Enforcement of Message or Data Structure	03-06-2020	5	In nghttp2 before version 1.41.0, the overly large HTTP/2 SETTINGS frame payload causes denial of service. The proof of concept attack involves a malicious client constructing a SETTINGS frame with a length of 14,400 bytes (2400 individual settings entries) over and over again. The attack causes the CPU to spike at 100%. nghttp2 v1.41.0 fixes this vulnerability. There is a workaround to this vulnerability. Implement nghttp2_on_frame_recv_callback callback, and if received frame is SETTINGS frame and the number of settings	https://github.com/nghttp2/nghttp2/security/advisories/GHSA-q5wr-xfw9-q7xr	A-NGH-NGHT-060820/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			entries are large (e.g., > 32), then drop the connection. **CVE ID : CVE-2020-11080**		
node-extend_project					
node-extend					
Improper Input Validation	10-06-2020	7.5	node-extend through 0.2.0 is vulnerable to Arbitrary Code Execution. User input provided to the argument `A` of `extend` function`(A,B,as,isAargs)` located within `lib/extend.js` is executed by the `eval` function, resulting in code execution. **CVE ID : CVE-2020-7673**	N/A	A-NOD-NODE-060820/468
Nodejs					
node.js					
Improper Certificate Validation	08-06-2020	5.8	TLS session reuse can lead to host certificate verification bypass in node version < 12.18.0 and < 14.4.0. **CVE ID : CVE-2020-8172**	https://security.netapp.com/advisory/ntap-20200625-0002/	A-NOD-NODE-060820/469
nozbe					
watermelondb					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-06-2020	5.5	In WatermelonDB (NPM package "@nozbe/watermelondb") before versions 0.15.1 and 0.16.2, a maliciously crafted record ID can exploit a SQL Injection vulnerability in iOS adapter implementation and cause the app to delete all or selected records from the database, generally causing the app to become unusable.	https://github.com/Nozbe/WatermelonDB/security/advisories/GHSA-38f9-m297-6q9g	A-NOZ-WATE-060820/470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This may happen in apps that don't validate IDs (valid IDs are `/^[a-zA-Z0-9_-.]+$/`) and use Watermelon Sync or low-level `database.adapter.destroyDeletedRecords` method. The integrity risk is low due to the fact that maliciously deleted records won't synchronize, so logout-login will restore all data, although some local changes may be lost if the malicious deletion causes the sync process to fail to proceed to push stage. No way to breach confidentiality with this vulnerability is known. Full exploitation of SQL Injection is mitigated, because it's not possible to nest an insert/update query inside a delete query in SQLite, and it's not possible to pass a semicolon-separated second query. There's also no known practicable way to breach confidentiality by selectively deleting records, because those records will not be synchronized. It's theoretically possible that selective record deletion could cause an app to behave insecurely if lack of a record is used to make security decisions by the app. This is patched in versions 0.15.1, 0.16.2, and 0.16.1-fix **CVE ID : CVE-2020-4035**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NTP					
ntp					
Improper Input Validation	04-06-2020	5.8	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets. The victim must be relying on unauthenticated IPv4 time sources. There must be an off-path attacker who can query time from the victim's ntpd instance. **CVE ID : CVE-2020-13817**	https://security.netapp.com/advisory/ntap-20200625-0004/	A-NTP-NTP-060820/471
Octobercms					
debugbar					
Information Exposure Through Log Files	04-06-2020	6.8	The October CMS debugbar plugin before version 3.1.0 contains a feature where it will log all requests (and all information pertaining to each request including session data) whenever it is enabled. This presents a problem if the plugin is ever enabled on a system that is open to untrusted users as the potential exists for them to use this feature to view all requests being made to the application and obtain sensitive information from those requests. There even exists the potential for account takeovers of authenticated users by non-	https://github.com/rainlab/debugbar-plugin/security/advisories/GHSA-c8wh-6jw4-2h79	A-OCT-DEBU-060820/472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated public users, which would then lead to a number of other potential issues as an attacker could theoretically get full access to the system if the required conditions existed. Issue has been patched in v3.1.0 by locking down access to the debugbar to all users; it now requires an authenticated backend user with a specifically enabled permission before it is even usable, and the feature that allows access to stored request information is restricted behind a different permission that's more restrictive. **CVE ID : CVE-2020-11094**		
october					
Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	03-06-2020	4	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to read local files of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466). **CVE ID : CVE-2020-5295**	https://github.com/octobercms/october/security/advisories/GHSA-r23f-c2j5-rx2f	A-OCT-OCTO-060820/473
External Control of	03-06-2020	4	In OctoberCMS (october/october composer	https://github.com/oct	A-OCT-OCTO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
File Name or Path			package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to delete arbitrary local files of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466). **CVE ID : CVE-2020-5296**	obercms/october/security/advisories/GHSA-jv6v-fvvx-4932	060820/474
External Control of File Name or Path	03-06-2020	4	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to upload jpg, jpeg, bmp, png, webp, gif, ico, css, js, woff, woff2, svg, ttf, eot, json, md, less, sass, scss, xml files to any directory of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466). **CVE ID : CVE-2020-5297**	https://github.com/obercms/october/security/advisories/GHSA-9722-rr68-rfpg	A-OCT-OCTO-060820/475
Improper Neutralization of Alternate XSS Syntax	03-06-2020	3.5	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, a user with the ability to use	https://github.com/obercms/october/security/advisori	A-OCT-OCTO-060820/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the import functionality of the `ImportExportController` behavior can be socially engineered by an attacker to upload a maliciously crafted CSV file which could result in a reflected XSS attack on the user in question Issue has been patched in Build 466 (v1.0.466). **CVE ID : CVE-2020-5298**	es/GHSA-gg6x-xx78-448c	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-06-2020	4.6	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, any users with the ability to modify any data that could eventually be exported as a CSV file from the `ImportExportController` could potentially introduce a CSV injection into the data to cause the generated CSV export file to be malicious. This requires attackers to achieve the following before a successful attack can be completed: 1. Have found a vulnerability in the victims spreadsheet software of choice. 2. Control data that would potentially be exported through the `ImportExportController` by a theoretical victim. 3. Convince the victim to export above data as a CSV and run it in vulnerable spreadsheet software while also bypassing any sanity	https://github.com/octobercms/october/security/advisories/GHSA-4rhm-m2fp-hx7q	A-OCT-OCTO-060820/477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			checks by said software. Issue has been patched in Build 466 (v1.0.466). **CVE ID : CVE-2020-5299**		
ohler					
agoo					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	10-06-2020	5	agoo through 2.12.3 allows request smuggling attacks where agoo is used as a backend and a frontend proxy also being vulnerable. It is possible to conduct HTTP request smuggling attacks by sending the Content-Length header twice. Furthermore, invalid Transfer Encoding headers were found to be parsed as valid which could be leveraged for TE:CL smuggling attacks. **CVE ID : CVE-2020-7670**	N/A	A-OHL-AGOO-060820/478
openbmc-project					
openbmc					
Incorrect Default Permissions	15-06-2020	6.5	user_channel/passwd_mgr.cpp in OpenBMC phosphor-host-ipmid before 2020-04-03 does not ensure that /etc/ipmi-pass has strong file permissions. **CVE ID : CVE-2020-14156**	https://github.com/openbmc/openbmc/issues/3670, https://lists.ozlabs.org/pipermail/openbmc/2020-June/022020.html	A-OPE-OPEN-060820/479
openbrowser_project					
openbrowser					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	08-06-2020	5.8	OpenSearch Web browser 1.0.4.9 allows Intent Scheme Hijacking.[a link that opens another app in the browser can be manipulated] **CVE ID : CVE-2020-8954**	N/A	A-OPE-OPEN-060820/480
Openbsd					
openssh					
Improper Input Validation	01-06-2020	5	** DISPUTED ** The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that "this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol" and "utimes does not fail under normal circumstances." **CVE ID : CVE-2020-12062**	N/A	A-OPE-OPEN-060820/481
Opencart					
opencart					
Improper Neutralization of Input	09-06-2020	3.5	** DISPUTED ** OpenCart 3.0.3.3 allows remote authenticated users to	N/A	A-OPE-OPEN-060820/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			conduct XSS attacks via a crafted filename in the users' image upload section because of a lack of entity encoding. NOTE: this issue exists because of an incomplete fix for CVE-2020-10596. The vendor states "this is not a massive issue as you are still required to be logged into the admin." **CVE ID : CVE-2020-13980**		
openjsf					
dijit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-06-2020	3.5	In Dijit before versions 1.11.11, and greater than or equal to 1.12.0 and less than 1.12.9, and greater than or equal to 1.13.0 and less than 1.13.8, and greater than or equal to 1.14.0 and less than 1.14.7, and greater than or equal to 1.15.0 and less than 1.15.4, and greater than or equal to 1.16.0 and less than 1.16.3, there is a cross-site scripting vulnerability in the Editor's LinkDialog plugin. This has been fixed in 1.11.11, 1.12.9, 1.13.8, 1.14.7, 1.15.4, 1.16.3. **CVE ID : CVE-2020-4051**	https://github.com/dojo/dijit/security/advisories/GHSA-cxjc-r2fp-7mq6	A-OPE-DIJI-060820/483
Opensuse					
backports_sle					
Incorrect Permission Assignment for Critical	08-06-2020	3.6	An issue was discovered in LinuxTV xawtv before 3.107. The function dev_open() in v4l-conf.c does not perform sufficient checks to prevent	http://www.openwall.com/lists/oss-security/20	A-OPE-BACK-060820/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource			an unprivileged caller of the program from opening unintended filesystem paths. This allows a local attacker with access to the v4l-conf setuid-root program to test for the existence of arbitrary files and to trigger an open on arbitrary files with mode O_RDWR. To achieve this, relative path components need to be added to the device path, as demonstrated by a v4l-conf -c /dev/../root/.bash_history command. **CVE ID : CVE-2020-13696**	20/06/04/6	
Open-xchange					
ox_guard					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-06-2020	4.3	OX Guard 2.10.3 and earlier allows XSS. **CVE ID : CVE-2020-9426**	N/A	A-OPE-OX_G-060820/485
Server-Side Request Forgery (SSRF)	15-06-2020	4	OX Guard 2.10.3 and earlier allows SSRF. **CVE ID : CVE-2020-9427**	N/A	A-OPE-OX_G-060820/486
Otrs					
otrs					
Information Exposure	08-06-2020	4.3	BCC recipients in mails sent from OTRS are visible in article detail on external interface. This issue affects OTRS: 8.0.3 and prior versions, 7.0.17 and prior	N/A	A-OTR-OTRS-060820/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions. **CVE ID : CVE-2020-1775**		
Owasp					
json-sanitizer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	4.3	OWASP json-sanitizer before 1.2.1 allows XSS. An attacker who controls a substring of the input JSON, and controls another substring adjacent to a SCRIPT element in which the output is embedded as JavaScript, may be able to confuse the HTML parser as to where the SCRIPT element ends, and cause non-script content to be interpreted as JavaScript. **CVE ID : CVE-2020-13973**	N/A	A-OWA-JSON-060820/488
p5-crypt-perl_project					
p5-crypt-perl					
Improper Verification of Cryptographic Signature	07-06-2020	6.8	Crypt::Perl::ECDSA in the Crypt::Perl (aka p5-Crypt-Perl) module before 0.32 for Perl fails to verify correct ECDSA signatures when r and s are small and when s = 1. This happens when using the curve secp256r1 (prime256v1). This could conceivably have a security-relevant impact if an attacker wishes to use public r and s values when guessing whether signature verification will fail. **CVE ID : CVE-2020-13895**	N/A	A-P5--P5-C-060820/489
Paloaltonetworks					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
globalprotect					
Time-of-check Time-of-use (TOCTOU) Race Condition	10-06-2020	6.9	A race condition vulnerability Palo Alto Networks GlobalProtect app on Windows allows a local limited Windows user to execute programs with SYSTEM privileges. This issue can be exploited only while performing a GlobalProtect app upgrade. This issue affects: GlobalProtect app 5.0 versions earlier than GlobalProtect app 5.0.10 on Windows; GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.4 on Windows. **CVE ID : CVE-2020-2032**	N/A	A-PAL-GLOB-060820/490
Improper Certificate Validation	10-06-2020	2.9	When the pre-logon feature is enabled, a missing certification validation in Palo Alto Networks GlobalProtect app can disclose the pre-logon authentication cookie to a man-in-the-middle attacker on the same local area network segment with the ability to manipulate ARP or to conduct ARP spoofing attacks. This allows the attacker to access the GlobalProtect Server as allowed by configured Security rules for the 'pre-login' user. This access may be limited compared to the network access of regular	N/A	A-PAL-GLOB-060820/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users. This issue affects: GlobalProtect app 5.0 versions earlier than GlobalProtect app 5.0.10 when the prelogon feature is enabled; GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.4 when the prelogon feature is enabled. **CVE ID : CVE-2020-2033**		
pam_tacplus_project					
pam_tacplus					
Information Exposure Through Log Files	06-06-2020	4.3	In support.c in pam_tacplus 1.3.8 through 1.5.1, the TACACS+ shared secret gets logged via syslog if the DEBUG loglevel and journald are used. **CVE ID : CVE-2020-13881**	N/A	A-PAM-PAM_-060820/492
Pandorafms					
pandora_fms					
Missing Authorization	11-06-2020	5	Artica Pandora FMS 7.44 has inadequate access controls on a web folder. **CVE ID : CVE-2020-13850**	N/A	A-PAN-PAND-060820/493
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	11-06-2020	9	Artica Pandora FMS 7.44 allows remote command execution via the events feature. **CVE ID : CVE-2020-13851**	N/A	A-PAN-PAND-060820/494
Unrestricted Upload of File with	11-06-2020	9	Artica Pandora FMS 7.44 allows arbitrary file upload (leading to remote command	N/A	A-PAN-PAND-060820/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			execution) via the File Manager feature. **CVE ID : CVE-2020-13852**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-06-2020	3.5	Artica Pandora FMS 7.44 has persistent XSS in the Messages feature. **CVE ID : CVE-2020-13853**	N/A	A-PAN-PAND-060820/496
Improper Privilege Management	11-06-2020	10	Artica Pandora FMS 7.44 allows privilege escalation. **CVE ID : CVE-2020-13854**	N/A	A-PAN-PAND-060820/497
Unrestricted Upload of File with Dangerous Type	11-06-2020	9	Artica Pandora FMS 7.44 allows arbitrary file upload (leading to remote command execution) via the File Repository Manager feature. **CVE ID : CVE-2020-13855**	N/A	A-PAN-PAND-060820/498
Pcre					
pcre					
Integer Overflow or Wraparound	15-06-2020	5	libpcre in PCRE before 8.44 allows an integer overflow via a large number after a (?C substring. **CVE ID : CVE-2020-14155**	https://about.gitlab.com/releases/2020/07/01/security-release-13-1-2-release/	A-PCR-PCRE-060820/499
pengutronix					
barebox					
Out-of-bounds Read	07-06-2020	6.4	Pengutronix Barebox through v2020.05.0 has an out-of-bounds read in nfs_read_reply in net/nfs.c because a field of an	N/A	A-PEN-BARE-060820/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			incoming network packet is directly used as a length field without any bounds check. **CVE ID : CVE-2020-13910**		
Perl					
Perl					
Integer Overflow or Wraparound	05-06-2020	7.5	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection. **CVE ID : CVE-2020-10878**	https://github.com/Perl/perl5/blob/blead/pod/perl5303delta.pod, https://github.com/perl/perl5/commit/0a320d753fe7fca03df259a4dfd8e641e51edaa8, https://github.com/perl/perl5/commit/3295b48defa0f8570114877b063fe546dd348b3c	A-PER-PERL-060820/501
Out-of-bounds Write	05-06-2020	6.4	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow. **CVE ID : CVE-2020-10543**	https://github.com/Perl/perl5/blob/blead/pod/perl5303delta.pod, https://github.com/perl/perl5/commit/897d1f7fd515b828e4b198d	A-PER-PERL-060820/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				8b8bef76c6faf03ed, https://github.com/Perl/perl5/compare/v5.30.2...v5.30.3	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	5	regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls. **CVE ID : CVE-2020-12723**	https://github.com/Perl/perl5/blob/blead/pod/perl5303delta.pod, https://github.com/perl/perl5/commit/66bbb51b93253a3f87d11c2695cfb7bdb782184a, https://github.com/Perl/perl5/compare/v5.30.2...v5.30.3	A-PER-PERL-060820/503
Philips					
intellibridge_enterprise					
Information Exposure Through Log Files	11-06-2020	2.7	Philips IntelliBridge Enterprise (IBE), Versions B.12 and prior, IntelliBridge Enterprise system integration with SureSigns (VS4), EarlyVue (VS30) and IntelliVue Guardian (IGS). Unencrypted user credentials received in the IntelliBridge Enterprise (IBE) are logged within the transaction logs, which are	N/A	A-PHI-INTE-060820/504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			secured behind the login based administrative web portal. The unencrypted user credentials sent from the affected products listed above, for the purpose of handshake or authentication with the Enterprise Systems, are logged as the payload in IntelliBridge Enterprise (IBE) within the transaction logs. An attacker with administrative privileges could exploit this vulnerability to read plain text credentials from log files. **CVE ID : CVE-2020-12023**		
Phplist					
phplist					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-06-2020	4.3	phpList before 3.5.4 allows XSS via /lists/admin/user.php and /lists/admin/users.php. **CVE ID : CVE-2020-13827**	N/A	A-PHP-PHPL-060820/505
phpmailer_project					
phpmailer					
Improper Encoding or Escaping of Output	08-06-2020	5	PHPMailer before 6.1.6 contains an output escaping bug when the name of a file attachment contains a double quote character. This can result in the file type being misinterpreted by the receiver or any mail relay processing the message.	https://github.com/PHPMailer/PHPMailer/releases/tag/v6.1.6, https://github.com/PHPMailer/PH	A-PHP-PHPM-060820/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13625	PMailer/security/advisories/GHSA-f7hx-fqxw-rvvj	
phpmussel_project					
phpmussel					
Deserialization of Untrusted Data	10-06-2020	7.5	phpMussel from versions 1.0.0 and less than 1.6.0 has an unserialization vulnerability in PHP's phar wrapper. Uploading a specially crafted file to an affected version allows arbitrary code execution (discovered, tested, and confirmed by myself), so the risk factor should be regarded as very high. Newer phpMussel versions don't use PHP's phar wrapper, and are therefore unaffected. This has been fixed in version 1.6.0. **CVE ID : CVE-2020-4043**	https://github.com/phpMussel/phpMussel/security/advisories/GHSA-qr95-4mq5-r3fh	A-PHP-PHPM-060820/507
pivotal_software					
spring_batch					
Deserialization of Untrusted Data	11-06-2020	6.8	When configured to enable default typing, Jackson contained a deserialization vulnerability that could lead to arbitrary code execution. Jackson fixed this vulnerability by blacklisting known "deserialization gadgets". Spring Batch configures Jackson with global default typing enabled which means that through	https://tanzu.vmware.com/security/cve-2020-5411	A-PIV-SPRI-060820/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the previous exploit, arbitrary code could be executed if all of the following is true: * Spring Batch's Jackson support is being leveraged to serialize a job's ExecutionContext. * A malicious user gains write access to the data store used by the JobRepository (where the data to be deserialized is stored). In order to protect against this type of attack, Jackson prevents a set of untrusted gadget classes from being deserialized. Spring Batch should be proactive against blocking unknown "deserialization gadgets" when enabling default typing. **CVE ID : CVE-2020-5411**		
playtube					
playtube					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-06-2020	4	PlayTube 1.8 allows disclosure of user details via ajax.php?type=../admin-panel/autoload&page=manage-users directory traversal, aka local file inclusion. **CVE ID : CVE-2020-13792**	N/A	A-PLA-PLAY-060820/509
Plex					
media_server					
Exposure of Resource to Wrong Sphere	15-06-2020	6.8	Improper Access Control in Plex Media Server prior to June 15, 2020 allows any origin to execute cross-origin application requests.	N/A	A-PLE-MEDI-060820/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5742		
Postgresql					
postgresql_jdbc_driver					
Improper Restriction of XML External Entity Reference ('XXE')	04-06-2020	6.8	PostgreSQL JDBC Driver (aka PgJDBC) before 42.2.13 allows XXE. **CVE ID : CVE-2020-13692**	https://github.com/pgjdbc/pgjdbc/commit/14b62aca4764d496813f55a43d050b017e01eb65, https://jdbc.postgresql.org/documentation/changelog.html#version_42.2.13, https://security.netapp.com/advisory/ntap-20200619-0005/	A-POS-POST-060820/511
prisma					
graphql-playground-html					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-06-2020	4.3	GraphQL Playground (graphql-playground-html NPM package) before version 1.6.22 have a severe XSS Reflection attack vulnerability. All unsanitized user input passed into renderPlaygroundPage() method could trigger this vulnerability. This has been patched in graphql-playground-html version	https://github.com/prisma-labs/graphql-playground/security/advisories/GHSA-4852-vrh7-28rf	A-PRI-GRAP-060820/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.6.22. Note that some of the associated dependent middleware packages are also affected including but not limited to graphql-playground-middleware-express before version 1.7.16, graphql-playground-middleware-koa before version 1.6.15, graphql-playground-middleware-lambda before version 1.7.17, and graphql-playground-middleware-hapi before 1.6.13. **CVE ID : CVE-2020-4038**		
graphql-playground-middleware-express					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-06-2020	4.3	GraphQL Playground (graphql-playground-html NPM package) before version 1.6.22 have a severe XSS Reflection attack vulnerability. All unsanitized user input passed into renderPlaygroundPage() method could trigger this vulnerability. This has been patched in graphql-playground-html version 1.6.22. Note that some of the associated dependent middleware packages are also affected including but not limited to graphql-playground-middleware-express before version 1.7.16, graphql-playground-middleware-koa before version 1.6.15, graphql-playground-middleware-	https://github.com/prisma-labs/graphql-playground/security/advisories/GHSA-4852-vrh7-28rf	A-PRI-GRAP-060820/513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lambda before version 1.7.17, and graphql-playground-middleware-hapi before 1.6.13. **CVE ID : CVE-2020-4038**		
graphql-playground-middleware-hapi					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-06-2020	4.3	GraphQL Playground (graphql-playground-html NPM package) before version 1.6.22 have a severe XSS Reflection attack vulnerability. All unsanitized user input passed into renderPlaygroundPage() method could trigger this vulnerability. This has been patched in graphql-playground-html version 1.6.22. Note that some of the associated dependent middleware packages are also affected including but not limited to graphql-playground-middleware-express before version 1.7.16, graphql-playground-middleware-koa before version 1.6.15, graphql-playground-middleware-lambda before version 1.7.17, and graphql-playground-middleware-hapi before 1.6.13. **CVE ID : CVE-2020-4038**	https://github.com/prisma-labs/graphql-playground/security/advisories/GHSA-4852-vrh7-28rf	A-PRI-GRAP-060820/514
graphql-playground-middleware-koa					
Improper Neutralization of Input During Web	08-06-2020	4.3	GraphQL Playground (graphql-playground-html NPM package) before version 1.6.22 have a severe	https://github.com/prisma-labs/graph	A-PRI-GRAP-060820/515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			XSS Reflection attack vulnerability. All unsanitized user input passed into renderPlaygroundPage() method could trigger this vulnerability. This has been patched in graphql-playground-html version 1.6.22. Note that some of the associated dependent middleware packages are also affected including but not limited to graphql-playground-middleware-express before version 1.7.16, graphql-playground-middleware-koa before version 1.6.15, graphql-playground-middleware-lambda before version 1.7.17, and graphql-playground-middleware-hapi before 1.6.13. **CVE ID : CVE-2020-4038**	ql-playground/security/advisories/GHSA-4852-vrh7-28rf	
graphql-playground-middleware-lambda					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-06-2020	4.3	GraphQL Playground (graphql-playground-html NPM package) before version 1.6.22 have a severe XSS Reflection attack vulnerability. All unsanitized user input passed into renderPlaygroundPage() method could trigger this vulnerability. This has been patched in graphql-playground-html version 1.6.22. Note that some of the associated dependent middleware packages are	https://github.com/prisma-labs/graphql-playground/security/advisories/GHSA-4852-vrh7-28rf	A-PRI-GRAP-060820/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			also affected including but not limited to graphql-playground-middleware-express before version 1.7.16, graphql-playground-middleware-koa before version 1.6.15, graphql-playground-middleware-lambda before version 1.7.17, and graphql-playground-middleware-hapi before 1.6.13. **CVE ID : CVE-2020-4038**		
projectcalico					
calico					
Information Exposure	03-06-2020	2.1	Clusters using Calico (version 3.14.0 and below), Calico Enterprise (version 2.8.2 and below), may be vulnerable to information disclosure if IPv6 is enabled but unused. A compromised pod with sufficient privilege is able to reconfigure the node's IPv6 interface due to the node accepting route advertisement by default, allowing the attacker to redirect full or partial network traffic from the node to the compromised pod. **CVE ID : CVE-2020-13597**	https://github.com/kubernetes/kubernetes/issues/91507, https://groups.google.com/forum/#!topic/kubernetes-security-announce/BMb_6ICCfp8, https://www.projectcalico.org/security-bulletins/	A-PRO-CALI-060820/517
Pydio					
cells					
Improper Privilege	11-06-2020	6.9	The following vulnerability applies only to the Pydio	N/A	A-PYD-CELL-060820/518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Cells Enterprise OVF version 2.0.4. Prior versions of the Pydio Cells Enterprise OVF (such as version 2.0.3) have a looser policy restriction allowing the "pydio" user to execute any privileged command using sudo. In version 2.0.4 of the appliance, the user pydio is responsible for running all the services and binaries that are contained in the Pydio Cells web application package, such as mysqld, cells, among others. This user has privileges restricted to run those services and nothing more. **CVE ID : CVE-2020-12850**		
Information Exposure	04-06-2020	5.5	Pydio Cells 2.0.4 allows an authenticated user to write or overwrite existing files in another user's personal and cells folders (repositories) by uploading a custom generated ZIP file and leveraging the file extraction feature present in the web application. The extracted files will be placed in the targeted user folders. **CVE ID : CVE-2020-12851**	N/A	A-PYD-CELL-060820/519
Improper Input Validation	04-06-2020	8.5	The update feature for Pydio Cells 2.0.4 allows an administrator user to set a custom update URL and the public RSA key used to validate the downloaded update package. The update	N/A	A-PYD-CELL-060820/520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process involves downloading the updated binary file from a URL indicated in the update server response, validating its checksum and signature with the provided public key and finally replacing the current application binary. To complete the update process, the application's service or appliance needs to be restarted. An attacker with administrator access can leverage the software update feature to force the application to download a custom binary that will replace current Pydio Cells binary. When the server or service is eventually restarted the attacker will be able to execute code under the privileges of the user running the application. In the Pydio Cells enterprise appliance this is with the privileges of the user named "pydio". **CVE ID : CVE-2020-12852**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-06-2020	4.3	Pydio Cells 2.0.4 allows XSS. A malicious user can either upload or create a new file that contains potentially malicious HTML and JavaScript code to personal folders or accessible cells. **CVE ID : CVE-2020-12853**	N/A	A-PYD-CELL-060820/521
Improper Input	04-06-2020	6.5	Pydio Cells 2.0.4 web application offers an	N/A	A-PYD-CELL-060820/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			administrative console named “Cells Console” that is available to users with an administrator role. This console provides an administrator user with the possibility of changing several settings, including the application’s mailer configuration. It is possible to configure a few engines to be used by the mailer application to send emails. If the user selects the “sendmail” option as the default one, the web application offers to edit the full path where the sendmail binary is hosted. Since there is no restriction in place while editing this value, an attacker authenticated as an administrator user could force the web application into executing any arbitrary binary. **CVE ID : CVE-2020-12847**		
Incorrect Permission Assignment for Critical Resource	05-06-2020	5.8	In Pydio Cells 2.0.4, once an authenticated user shares a file selecting the create a public link option, a hidden shared user account is created in the backend with a random username. An anonymous user that obtains a valid public link can get the associated hidden account username and password and proceed to login to the web application. Once logged into the web application with the	N/A	A-PYD-CELL-060820/523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hidden user account, some actions that were not available with the public share link can now be performed. **CVE ID : CVE-2020-12848**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-06-2020	3.5	Pydio Cells 2.0.4 allows any user to upload a profile image to the web application, including standard and shared user roles. These profile pictures can later be accessed directly with the generated URL by any unauthenticated or authenticated user. **CVE ID : CVE-2020-12849**	N/A	A-PYD-CELL-060820/524
python-rsa_project					
python-rsa					
Use of a Broken or Risky Cryptographic Algorithm	01-06-2020	5	Python-RSA before 4.1 ignores leading '\0' bytes during decryption of ciphertext. This could conceivably have a security-relevant impact, e.g., by helping an attacker to infer that an application uses Python-RSA, or if the length of accepted ciphertext affects application behavior (such as by causing excessive memory allocation). **CVE ID : CVE-2020-13757**	https://github.com/sybrenstuvel/python-rsa/issues/146#issuecomment-641845667	A-PYT-PYTH-060820/525
Qbik					
wingate					
Incorrect Default	08-06-2020	7.2	WinGate v9.4.1.5998 has insecure permissions for the	N/A	A-QBI-WING-060820/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			installation directory, which allows local users to gain privileges by replacing an executable file with a Trojan horse. **CVE ID : CVE-2020-13866**		
Qemu					
qemu					
N/A	04-06-2020	2.1	A flaw was found in QEMU in the implementation of the Pointer Authentication (PAuth) support for ARM introduced in version 4.0 and fixed in version 5.0.0. A general failure of the signature generation process caused every PAuth-enforced pointer to be signed with the same signature. A local attacker could obtain the signature of a protected pointer and abuse this flaw to bypass PAuth protection for all programs running on QEMU. **CVE ID : CVE-2020-10702**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10702, https://git.qemu.org/?p=qemu.git;a=commit;h=de0b1bae6461f6724328255475f88b2384a1eb9	A-QEM-QEMU-060820/527
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	hw/pci/msix.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access via a crafted address in an msi-x mmio operation. **CVE ID : CVE-2020-13754**	http://www.openwall.com/lists/oss-security/2020/06/01/6, https://security.netapp.com/advisory/ntap-20200608-0007/	A-QEM-QEMU-060820/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-06-2020	6.8	rom_copy() in hw/core/loader.c in QEMU 4.1.0 does not validate the relationship between two addresses, which allows attackers to trigger an invalid memory copy operation. **CVE ID : CVE-2020-13765**	https://security.netapp.com/advisory/ntap-20200619-0006/, https://www.openwall.com/lists/oss-security/2020/06/03/6	A-QEM-QEMU-060820/529
Out-of-bounds Read	04-06-2020	2.1	hw/pci/pci.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access by providing an address near the end of the PCI configuration space. **CVE ID : CVE-2020-13791**	https://security.netapp.com/advisory/ntap-20200717-0001/, https://www.openwall.com/lists/oss-security/2020/06/04/1	A-QEM-QEMU-060820/530
Reachable Assertion	09-06-2020	4	An assertion failure issue was found in the Network Block Device(NBD) Server in all QEMU versions before QEMU 5.0.1. This flaw occurs when an nbd-client sends a spec-compliant request that is near the boundary of maximum permitted request length. A remote nbd-client could use this flaw to crash the qemu-nbd server resulting in a denial of service.	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10761	A-QEM-QEMU-060820/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10761		
NULL Pointer Dereference	02-06-2020	1.9	address_space_map in exec.c in QEMU 4.2.0 can trigger a NULL pointer dereference related to BounceBuffer. **CVE ID : CVE-2020-13659**	http://www.openwall.com/lists/oss-security/2020/06/01/3, https://security.netapp.com/advisory/ntap-20200608-0007/	A-QEM-QEMU-060820/532
Loop with Unreachable Exit Condition ('Infinite Loop')	04-06-2020	4.9	ati-vga in hw/display/ati.c in QEMU 4.2.0 allows guest OS users to trigger infinite recursion via a crafted mm_index value during an ati_mm_read or ati_mm_write call. **CVE ID : CVE-2020-13800**	https://security.netapp.com/advisory/ntap-20200717-0001/, https://www.openwall.com/lists/oss-security/2020/06/04/2	A-QEM-QEMU-060820/533
QT					
qt					
N/A	09-06-2020	5	Qt 5.12.2 through 5.14.2, as used in unofficial builds of Mumble 1.3.0 and other products, mishandles OpenSSL's error queue, which can cause a denial of service to QSslSocket users. Because errors leak in unrelated TLS sessions, an unrelated session may be disconnected when any	N/A	A-QT-QT-060820/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handshake fails. (Mumble 1.3.1 is not affected, regardless of the Qt version.) **CVE ID : CVE-2020-13962**		
quickbox					
quickbox					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-06-2020	9	QuickBox Community Edition through 2.5.5 and Pro Edition through 2.1.8 allows an authenticated remote attacker to execute code on the server via command injection in the servicestart parameter. **CVE ID : CVE-2020-13448**	N/A	A-QUI-QUIC-060820/535
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-06-2020	9	In QuickBox Community Edition through 2.5.5 and Pro Edition through 2.1.8, the local www-data user can execute sudo mysql without a password, which means that the www-data user can execute arbitrary OS commands via the mysql -e option. **CVE ID : CVE-2020-13694**	N/A	A-QUI-QUIC-060820/536
Improper Privilege Management	01-06-2020	9	In QuickBox Community Edition through 2.5.5 and Pro Edition through 2.1.8, the local www-data user has sudo privileges to execute grep as root without a password, which allows an attacker to obtain sensitive information via a grep of a /root/*.db or /etc/shadow file. **CVE ID : CVE-2020-13695**	N/A	A-QUI-QUIC-060820/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
rconfig					
rconfig					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-06-2020	7.5	rConfig 3.9.4 and previous versions has unauthenticated compliancepolicies.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices. **CVE ID : CVE-2020-10546**	N/A	A-RCO-RCON-060820/538
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-06-2020	7.5	rConfig 3.9.4 and previous versions has unauthenticated compliancepolicyelements.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices. **CVE ID : CVE-2020-10547**	N/A	A-RCO-RCON-060820/539
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-06-2020	7.5	rConfig 3.9.4 and previous versions has unauthenticated devices.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices. **CVE ID : CVE-2020-10548**	N/A	A-RCO-RCON-060820/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-06-2020	7.5	rConfig 3.9.4 and previous versions has unauthenticated snippets.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices. **CVE ID : CVE-2020-10549**	N/A	A-RCO-RCON-060820/541
redash					
redash					
Server-Side Request Forgery (SSRF)	11-06-2020	6.5	Havoc Research discovered an authenticated Server-Side Request Forgery (SSRF) via the "JSON" data source of Redash open-source 8.0.0 and prior. Possibly, other connectors are affected. The SSRF is potent and provides a lot of flexibility in terms of being able to craft HTTP requests e.g., by adding headers, selecting any HTTP verb, etc. **CVE ID : CVE-2020-12725**	N/A	A-RED-REDA-060820/542
Redhat					
openshift_container_platform					
N/A	03-06-2020	6	A vulnerability was found in all versions of containernetworking/plugins before version 0.8.6, that allows malicious containers in Kubernetes clusters to perform man-in-the-middle (MitM) attacks. A malicious container can exploit this	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10749	A-RED-OPEN-060820/543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			flaw by sending rogue IPv6 router advertisements to the host or other containers, to redirect traffic to the malicious container. **CVE ID : CVE-2020-10749**		
Uncontrolled Resource Consumption	12-06-2020	6	A flaw was found in the OpenShift API Server, where it failed to sufficiently protect OAuthTokens by leaking them into the logs when an API Server panic occurred. This flaw allows an attacker with the ability to cause an API Server error to read the logs, and use the leaked OAuthToken to log into the API Server with the leaked token. **CVE ID : CVE-2020-10752**	https://github.com/openshift/enhancements/pull/323, https://github.com/openshift/origin/blob/master/vendor/k8s.io/kubernetes/staging/src/k8s.io/apiserver/pkg/server/filters/wrap.go#L39	A-RED-OPEN-060820/544
Improper Control of Generation of Code ('Code Injection')	03-06-2020	6.5	Kibana versions before 6.8.9 and 7.7.0 contain a prototype pollution flaw in TSVB. An authenticated attacker with privileges to create TSVB visualizations could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system. **CVE ID : CVE-2020-7013**	N/A	A-RED-OPEN-060820/545
libvirt					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-06-2020	4	A NULL pointer dereference was found in the libvirt API responsible introduced in upstream version 3.10.0, and fixed in libvirt 6.0.0, for fetching a storage pool based on its target path. In more detail, this flaw affects storage pools created without a target path such as network-based pools like gluster and RBD. Unprivileged users with a read-only connection could abuse this flaw to crash the libvirt daemon, resulting in a potential denial of service. **CVE ID : CVE-2020-10703**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10703, https://libvirt.org/git/?p=libvirt.git;a=commit;h=5d5c732d748d644ec14626bce448e84bdc4bd93e, https://libvirt.org/git/?p=libvirt.git;a=commit;h=7aa0e8c0cb8a6293d0c6f7e3d29c13b96dec2129	A-RED-LIBV-060820/546
undertow					
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-06-2020	5	A flaw was discovered in Undertow in versions before Undertow 2.1.1.Final where certain requests to the "Expect: 100-continue" header may cause an out of memory error. This flaw may potentially lead to a denial of service. **CVE ID : CVE-2020-10705**	N/A	A-RED-UNDE-060820/547
enterprise_mrg					
Improper Privilege Management	09-06-2020	6.9	A flaw was found in the Linux Kernel in versions after 4.5-rc1 in the way mremap handled DAX Huge	https://security.netapp.com/advisory/ntap-	A-RED-ENTE-060820/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Pages. This flaw allows a local attacker with access to a DAX enabled storage to escalate their privileges on the system. **CVE ID : CVE-2020-10757**	20200702-0004/	
openstack-cinder					
Insufficiently Protected Credentials	10-06-2020	4.3	An insecure-credentials flaw was found in all openstack-cinder versions before openstack-cinder 14.1.0, all openstack-cinder 15.x.x versions before openstack-cinder 15.2.0 and all openstack-cinder 16.x.x versions before openstack-cinder 16.1.0. When using openstack-cinder with the Dell EMC ScaleIO or VxFlex OS backend storage driver, credentials for the entire backend are exposed in the ``connection_info`` element in all Block Storage v3 Attachments API calls containing that element. This flaw enables an end-user to create a volume, make an API call to show the attachment detail information, and retrieve a username and password that may be used to connect to another user's volume. Additionally, these credentials are valid for the ScaleIO or VxFlex OS Management API, should an attacker discover the Management API endpoint.	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10755	A-RED-OPEN-060820/549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Source: OpenStack project **CVE ID : CVE-2020-10755**		
redislabs					
redis					
Integer Overflow or Wraparound	15-06-2020	4	An integer overflow in the getnum function in lua_struct.c in Redis before 6.0.3 allows context-dependent attackers with permission to run Lua code in a Redis session to cause a denial of service (memory corruption and application crash) or possibly bypass intended sandbox restrictions via a large number, which triggers a stack-based buffer overflow. NOTE: this issue exists because of a CVE-2015-8080 regression. **CVE ID : CVE-2020-14147**	N/A	A-RED-REDI-060820/550
Rejetto					
http_file_server					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-06-2020	5	rejetto HFS (aka HTTP File Server) v2.3m Build #300, when virtual files or folders are used, allows remote attackers to trigger an invalid-pointer write access violation via concurrent HTTP requests with a long URI or long HTTP headers. **CVE ID : CVE-2020-13432**	N/A	A-REJ-HTTP-060820/551
rocketgenius					
gravityforms					
Information	02-06-2020	5	common.php in the Gravity	N/A	A-ROC-GRAV-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Forms plugin before 2.4.9 for WordPress can leak hashed passwords because user_pass is not considered a special case for a $current_user->get($property) call. **CVE ID : CVE-2020-13764**		060820/552
Rockwellautomation					
rslinx_classic					
Improper Input Validation	15-06-2020	5.5	FactoryTalk Linx versions 6.00, 6.10, and 6.11, RSLinx Classic v4.11.00 and prior,Connected Components Workbench: Version 12 and prior, ControlFLASH: Version 14 and later, ControlFLASH Plus: Version 1 and later, FactoryTalk Asset Centre: Version 9 and later, FactoryTalk Linx CommDTM: Version 1 and later, Studio 5000 Launcher: Version 31 and later Stud, 5000 Logix Designer software: Version 32 and prior is vulnerable. An exposed API call allows users to provide files to be processed without sanitation. This may allow an attacker to specify a filename to execute unauthorized code and modify files or data. **CVE ID : CVE-2020-11999**	N/A	A-ROC-RSLI-060820/553
Improper Input	15-06-2020	7.5	FactoryTalk Linx versions 6.00, 6.10, and 6.11, RSLinx	N/A	A-ROC-RSLI-060820/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Classic v4.11.00 and prior,Connected Components Workbench: Version 12 and prior, ControlFLASH: Version 14 and later, ControlFLASH Plus: Version 1 and later, FactoryTalk Asset Centre: Version 9 and later, FactoryTalk Linx CommDTM: Version 1 and later, Studio 5000 Launcher: Version 31 and later Stud, 5000 Logix Designer software: Version 32 and prior is vulnerable. The parsing mechanism that processes certain file types does not provide input sanitation. This may allow an attacker to use specially crafted files to traverse the file system and modify or expose sensitive data or execute arbitrary code. **CVE ID : CVE-2020-12001**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-06-2020	5	FactoryTalk Linx versions 6.00, 6.10, and 6.11, RSLinx Classic v4.11.00 and prior,Connected Components Workbench: Version 12 and prior, ControlFLASH: Version 14 and later, ControlFLASH Plus: Version 1 and later, FactoryTalk Asset Centre: Version 9 and later, FactoryTalk Linx CommDTM: Version 1 and later, Studio 5000 Launcher: Version 31 and later Stud,	N/A	A-ROC-RSLI-060820/555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5000 Logix Designer software: Version 32 and prior is vulnerable. An exposed API call allows users to provide files to be processed without sanitation. This may allow an attacker to use specially crafted requests to traverse the file system and expose sensitive data on the local hard drive. **CVE ID : CVE-2020-12003**		
Unrestricted Upload of File with Dangerous Type	15-06-2020	7.8	FactoryTalk Linx versions 6.00, 6.10, and 6.11, RSLinx Classic v4.11.00 and prior,Connected Components Workbench: Version 12 and prior, ControlFLASH: Version 14 and later, ControlFLASH Plus: Version 1 and later, FactoryTalk Asset Centre: Version 9 and later, FactoryTalk Linx CommDTM: Version 1 and later, Studio 5000 Launcher: Version 31 and later Stud, 5000 Logix Designer software: Version 32 and prior is vulnerable. A vulnerability exists in the communication function that enables users to upload EDS files by FactoryTalk Linx. This may allow an attacker to upload a file with bad compression, consuming all the available CPU resources, leading to a denial-of-service	N/A	A-ROC-RSLI-060820/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. **CVE ID : CVE-2020-12005**		
factorytalk_linx					
Improper Input Validation	15-06-2020	5.5	FactoryTalk Linx versions 6.00, 6.10, and 6.11, RSLinx Classic v4.11.00 and prior,Connected Components Workbench: Version 12 and prior, ControlFLASH: Version 14 and later, ControlFLASH Plus: Version 1 and later, FactoryTalk Asset Centre: Version 9 and later, FactoryTalk Linx CommDTM: Version 1 and later, Studio 5000 Launcher: Version 31 and later Stud, 5000 Logix Designer software: Version 32 and prior is vulnerable. An exposed API call allows users to provide files to be processed without sanitation. This may allow an attacker to specify a filename to execute unauthorized code and modify files or data. **CVE ID : CVE-2020-11999**	N/A	A-ROC-FACT-060820/557
Improper Input Validation	15-06-2020	7.5	FactoryTalk Linx versions 6.00, 6.10, and 6.11, RSLinx Classic v4.11.00 and prior,Connected Components Workbench: Version 12 and prior, ControlFLASH: Version 14 and later, ControlFLASH Plus: Version 1 and later, FactoryTalk Asset Centre:	N/A	A-ROC-FACT-060820/558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Version 9 and later, FactoryTalk Linx CommDTM: Version 1 and later, Studio 5000 Launcher: Version 31 and later Stud, 5000 Logix Designer software: Version 32 and prior is vulnerable. The parsing mechanism that processes certain file types does not provide input sanitation. This may allow an attacker to use specially crafted files to traverse the file system and modify or expose sensitive data or execute arbitrary code. **CVE ID : CVE-2020-12001**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-06-2020	5	FactoryTalk Linx versions 6.00, 6.10, and 6.11, RSLinx Classic v4.11.00 and prior,Connected Components Workbench: Version 12 and prior, ControlFLASH: Version 14 and later, ControlFLASH Plus: Version 1 and later, FactoryTalk Asset Centre: Version 9 and later, FactoryTalk Linx CommDTM: Version 1 and later, Studio 5000 Launcher: Version 31 and later Stud, 5000 Logix Designer software: Version 32 and prior is vulnerable. An exposed API call allows users to provide files to be processed without sanitation. This may allow an attacker to use specially	N/A	A-ROC-FACT-060820/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted requests to traverse the file system and expose sensitive data on the local hard drive. **CVE ID : CVE-2020-12003**		
Unrestricted Upload of File with Dangerous Type	15-06-2020	7.8	FactoryTalk Linx versions 6.00, 6.10, and 6.11, RSLinx Classic v4.11.00 and prior,Connected Components Workbench: Version 12 and prior, ControlFLASH: Version 14 and later, ControlFLASH Plus: Version 1 and later, FactoryTalk Asset Centre: Version 9 and later, FactoryTalk Linx CommDTM: Version 1 and later, Studio 5000 Launcher: Version 31 and later Stud, 5000 Logix Designer software: Version 32 and prior is vulnerable. A vulnerability exists in the communication function that enables users to upload EDS files by FactoryTalk Linx. This may allow an attacker to upload a file with bad compression, consuming all the available CPU resources, leading to a denial-of-service condition. **CVE ID : CVE-2020-12005**	N/A	A-ROC-FACT-060820/560
Roundcube					
webmail					
Improper Neutralization of Input	09-06-2020	4.3	An issue was discovered in Roundcube Webmail before 1.3.12 and 1.4.x before 1.4.5.	https://roundcube.net/news/2020	A-ROU-WEBM-060820/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			include/rcmail_output_html.php allows XSS via the username template object. **CVE ID : CVE-2020-13964**	/06/02/security-updates-1.4.5-and-1.3.12	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	4.3	An issue was discovered in Roundcube Webmail before 1.3.12 and 1.4.x before 1.4.5. There is XSS via a malicious XML attachment because text/xml is among the allowed types for a preview. **CVE ID : CVE-2020-13965**	https://roundcube.net/news/2020/06/02/security-updates-1.4.5-and-1.3.12	A-ROU-WEBM-060820/562
royalapps					
royal_ts					
Improper Restriction of Excessive Authentication Attempts	09-06-2020	3.3	Royal TS before 5 has a 0.0.0.0 listener, which makes it easier for attackers to bypass tunnel authentication via a brute-force approach. **CVE ID : CVE-2020-13872**	N/A	A-ROY-ROYA-060820/563
sabberworm					
php_css_parser					
Improper Input Validation	03-06-2020	7.5	Sabberworm PHP CSS Parser before 8.3.1 calls eval on uncontrolled data, possibly leading to remote code execution if the function allSelectors() or getSelectorsBySpecificity() is called with input from an attacker. **CVE ID : CVE-2020-13756**	N/A	A-SAB-PHP_-060820/564
SAP					
commerce					
Information Exposure	10-06-2020	5	SAP Commerce, versions - 6.7, 1808, 1811, 1905, may	N/A	A-SAP-COMM-060820/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to access information under certain conditions which would otherwise be restricted, leading to Information Disclosure. **CVE ID : CVE-2020-6264**		
Use of Hard-coded Credentials	09-06-2020	7.5	SAP Commerce, versions - 6.7, 1808, 1811, 1905, and SAP Commerce (Data Hub), versions - 6.7, 1808, 1811, 1905, allows an attacker to bypass the authentication and/or authorization that has been configured by the system administrator due to the use of Hardcoded Credentials. **CVE ID : CVE-2020-6265**	N/A	A-SAP-COMM-060820/566
commerce_data_hub					
Use of Hard-coded Credentials	09-06-2020	7.5	SAP Commerce, versions - 6.7, 1808, 1811, 1905, and SAP Commerce (Data Hub), versions - 6.7, 1808, 1811, 1905, allows an attacker to bypass the authentication and/or authorization that has been configured by the system administrator due to the use of Hardcoded Credentials. **CVE ID : CVE-2020-6265**	N/A	A-SAP-COMM-060820/567
fiori					
URL Redirection to Untrusted Site ('Open Redirect')	10-06-2020	4.9	SAP Fiori for SAP S/4HANA, versions - 100, 200, 300, 400, allows an attacker to redirect users to a malicious site due to insufficient URL validation, leading to URL	N/A	A-SAP-FIOR-060820/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Redirection. **CVE ID : CVE-2020-6266**		
erp_\(ea-finserv\)					
Missing Authorization	10-06-2020	5.5	Statutory Reporting for Insurance Companies in SAP ERP (EA-FINSERV versions - 600, 603, 604, 605, 606, 616, 617, 618, 800 and S4CORE versions 101, 102, 103, 104) does not execute the required authorization checks for an authenticated user, allowing an attacker to view and tamper with certain restricted data leading to Missing Authorization Check. **CVE ID : CVE-2020-6268**	N/A	A-SAP-ERP_-060820/569
erp_\(s4core\)					
Missing Authorization	10-06-2020	5.5	Statutory Reporting for Insurance Companies in SAP ERP (EA-FINSERV versions - 600, 603, 604, 605, 606, 616, 617, 618, 800 and S4CORE versions 101, 102, 103, 104) does not execute the required authorization checks for an authenticated user, allowing an attacker to view and tamper with certain restricted data leading to Missing Authorization Check. **CVE ID : CVE-2020-6268**	N/A	A-SAP-ERP_-060820/570
successfactors_recruiting					
Incorrect Authorization	10-06-2020	6.5	OData APIs and JobApplicationInterview and JobApplication export	N/A	A-SAP-SUCC-060820/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permissions in SAP SuccessFactors Recruiting, version 2005, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2020-6279**		
solution_manager					
XML Injection (aka Blind XPath Injection)	10-06-2020	5	SAP Solution Manager (Trace Analysis), version 7.20, allows an attacker to inject superflous data that can be displayed by the application, due to Incomplete XML Validation. The application shows additional data that do not actually exist. **CVE ID : CVE-2020-6260**	N/A	A-SAP-SOLU-060820/572
XML Injection (aka Blind XPath Injection)	10-06-2020	5.5	SAP Solution Manager (Problem Context Manager), version 7.2, does not perform the necessary authentication, allowing an attacker to consume large amounts of memory, causing the system to crash and read restricted data (files visible for technical administration users of the diagnostics agent). **CVE ID : CVE-2020-6271**	N/A	A-SAP-SOLU-060820/573
business_one					
Information Exposure	10-06-2020	2.1	Under certain conditions SAP Business One (Backup service), versions 9.3, 10.0, allows an attacker with admin permissions to view	N/A	A-SAP-BUSI-060820/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SYSTEM user password in clear text, leading to Information Disclosure. **CVE ID : CVE-2020-6239**		
netweaver_as_abap_business_server_pages					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-06-2020	4.3	SAP NetWeaver AS ABAP Business Server Pages Test Application SBSPEXT_TABLE, versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, does not sufficiently encode user-controlled inputs, resulting in reflected Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2020-6246**	N/A	A-SAP-NETW-060820/575
netweaver_application_server_java					
Improper Authentication	10-06-2020	7.5	Standalone clients connecting to SAP NetWeaver AS Java via P4 Protocol, versions (SAP-JEECOR 7.00, 7.01; SERVERCOR 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50; CORE-TOOLS 7.00, 7.01, 7.02, 7.05, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50) do not perform any authentication checks for operations that require user identity leading to Authentication Bypass. **CVE ID : CVE-2020-6263**	N/A	A-SAP-NETW-060820/576
netweaver_as_abap					
Missing Authorization	10-06-2020	4	SAP NetWeaver AS ABAP (Banking Services), versions - 710, 711, 740, 750, 751, 752, 75A, 75B, 75C, 75D, 75E, does not perform	N/A	A-SAP-NETW-060820/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			necessary authorization checks for an authenticated user due to Missing Authorization Check, allowing wrong and unexpected change of individual conditions by a malicious user leading to wrong prices. **CVE ID : CVE-2020-6270**		
Server-Side Request Forgery (SSRF)	10-06-2020	6.8	SAP Netweaver AS ABAP, versions 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, are vulnerable for Server Side Request Forgery Attack where in an attacker can use inappropriate path names containing malicious server names in the import/export of sessions functionality and coerce the web server into authenticating with the malicious server. Furthermore, if NTLM is setup the attacker can compromise confidentiality, integrity and availability of the SAP database. **CVE ID : CVE-2020-6275**	N/A	A-SAP-NETW-060820/578
businessobjects_business_intelligence_platform					
Information Exposure	10-06-2020	4	Under certain conditions SAP Business Objects Business Intelligence Platform, version 4.2, allows an attacker to access information which would otherwise be restricted, leading to Information	N/A	A-SAP-BUSI-060820/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure. **CVE ID : CVE-2020-6269**		
scuttlebutt					
ssb-db					
Information Exposure	11-06-2020	5	SSB-DB version 20.0.0 has an information disclosure vulnerability. The get() method is supposed to only decrypt messages when you explicitly ask it to, but there is a bug where it's decrypting any message that it can. This means that it is returning the decrypted content of private messages, which a malicious peer could use to get access to private data. This only affects peers running SSB-DB@20.0.0 who also have private messages, and is only known to be exploitable if you're also running SSB-OOO (default in SSB-Server), which exposes a thin wrapper around get() to anonymous peers. This is fixed in version 20.0.1. Note that users of SSB-Server verion 16.0.0 should upgrade to 16.0.1 to get the fixed version of SSB-DB. **CVE ID : CVE-2020-4045**	https://github.com/ssbc/ssb-db/security/advisories/GHSA-mpgr-2cx9-327h	A-SCU-SSB--060820/580
Siemens					
simatic_wincc_runtime_advanced					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 <	N/A	A-SIE-SIMA-060820/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions),		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
simatic_automatic_tool					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime	N/A	A-SIE-SIMA-060820/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
simatic_net_pc					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC	N/A	A-SIE-SIMA-060820/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
simatic_pcs_neo					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional	N/A	A-SIE-SIMA-060820/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
simatic_prosave					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions),	N/A	A-SIE-SIMA-060820/585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
simatic_step_7					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14	N/A	A-SIE-SIMA-060820/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
Uncontrolled Search Path Element	10-06-2020	4.6	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3), SIMATIC PDM (All versions), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF1). A DLL Hijacking vulnerability could allow a local attacker to execute code with elevated privileges. The security	N/A	A-SIE-SIMA-060820/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information. **CVE ID : CVE-2020-7585**		
Out-of-bounds Write	10-06-2020	4.6	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3), SIMATIC PDM (All versions), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF1). A buffer overflow vulnerability could allow a local attacker to cause a Denial-of-Service situation. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information.	N/A	A-SIE-SIMA-060820/588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7586		
simatic_wincc_open_architecture					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC	N/A	A-SIE-SIMA-060820/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
sinamics_startdrive					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7	N/A	A-SIE-SINA-060820/590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
sinamics_starter_commissioning_tool					
Unquoted	10-06-2020	7.2	A vulnerability has been	N/A	A-SIE-SINA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Search Path or Element			identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1		060820/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
sinec_network_management_system					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16	N/A	A-SIE-SINE-060820/592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
sinumerik_one_virtual					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC	N/A	A-SIE-SINU-060820/593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
sinumerik_operate					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003),	N/A	A-SIE-SINU-060820/594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
simatic_process_device_manager					
Uncontrolled Search Path Element	10-06-2020	4.6	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3), SIMATIC PDM (All versions), SIMATIC STEP 7	N/A	A-SIE-SIMA-060820/595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF1). A DLL Hijacking vulnerability could allow a local attacker to execute code with elevated privileges. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information. **CVE ID : CVE-2020-7585**		
Out-of-bounds Write	10-06-2020	4.6	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3), SIMATIC PDM (All versions), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF1). A buffer overflow vulnerability could allow a local attacker to cause a Denial-of-Service situation. The security vulnerability could be exploited by an attacker with local access to the affected systems.	N/A	A-SIE-SIMA-060820/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information. **CVE ID : CVE-2020-7586**		
sinamics_starter					
Uncontrolled Search Path Element	10-06-2020	4.6	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3), SIMATIC PDM (All versions), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF1). A DLL Hijacking vulnerability could allow a local attacker to execute code with elevated privileges. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information. **CVE ID : CVE-2020-7585**	N/A	A-SIE-SINA-060820/597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-06-2020	4.6	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3), SIMATIC PDM (All versions), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF1). A buffer overflow vulnerability could allow a local attacker to cause a Denial-of-Service situation. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information. **CVE ID : CVE-2020-7586**	N/A	A-SIE-SINA-060820/598
simatic_pcs_7					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions),	N/A	A-SIE-SIMA-060820/599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
Uncontrolled Search Path Element	10-06-2020	4.6	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3), SIMATIC PDM (All versions), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF1). A DLL Hijacking vulnerability could allow a local attacker to execute code with elevated privileges. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information. **CVE ID : CVE-2020-7585**	N/A	A-SIE-SIMA-060820/600
Out-of-bounds Write	10-06-2020	4.6	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0	N/A	A-SIE-SIMA-060820/601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SP3), SIMATIC PDM (All versions), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF1). A buffer overflow vulnerability could allow a local attacker to cause a Denial-of-Service situation. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information. **CVE ID : CVE-2020-7586**		
simatic_wincc					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7	N/A	A-SIE-SIMA-060820/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7580		
simatic_wincc_runtime_professional					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC	N/A	A-SIE-SIMA-060820/603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
sinema_server					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7	N/A	A-SIE-SINE-060820/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
Solarwinds					
advanced_monitoring_agent					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	07-06-2020	6	SolarWinds Advanced Monitoring Agent before 10.8.9 allows local users to gain privileges via a Trojan horse .exe file, because everyone can write to a certain .exe file. **CVE ID : CVE-2020-13912**	N/A	A-SOL-ADVA-060820/605
sos-berlin					
jobscheduler					
Insufficiently Protected Credentials	11-06-2020	5	A vulnerability based on insecure user/password encryption in the JOE (job editor) component of SOS JobScheduler 1.12 and 1.13 allows attackers to decrypt the user/password that is optionally stored with a user's profile. **CVE ID : CVE-2020-12712**	https://change.sos-berlin.com/browse/JOE-290	A-SOS-JOBS-060820/606
Sqlite					
sqlite					
Use After Free	06-06-2020	5	SQLite 3.32.2 has a use-after-free in resetAccumulator in select.c because the parse tree rewrite for window functions is too late. **CVE ID : CVE-2020-13871**	https://security.netapp.com/advisory/ntap-20200619-0002/	A-SQL-SQLI-060820/607
synacor					
zimbra_collaboration_suite					
Unrestricted Upload of File with Dangerous Type	03-06-2020	6	Zimbra before 8.8.15 Patch 10 and 9.x before 9.0.0 Patch 3 allows remote code execution via an avatar file. There is potential abuse of /service/upload servlet in the webmail subsystem. A	https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P3	A-SYN-ZIMB-060820/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user can upload executable files (exe,sh,bat,jar) in the Contact section of the mailbox as an avatar image for a contact. A user will receive a "Corrupt File" error, but the file is still uploaded and stored locally in /opt/zimbra/data/tmp/upload/, leaving it open to possible remote execution. **CVE ID : CVE-2020-12846**		
synaptics					
smart_audio_uwp					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	A-SYN-SMAR-060820/609
Sysax					
multi_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-06-2020	5	An issue was discovered in Sysax Multi Server 6.90. An attacker can determine the username (under which the web server is running) by triggering an invalid path permission error. This bypasses the fakepath protection mechanism. **CVE ID : CVE-2020-13227**	N/A	A-SYS-MULT-060820/610
Improper	02-06-2020	4.3	An issue was discovered in	N/A	A-SYS-MULT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			Sysax Multi Server 6.90. There is reflected XSS via the /scgi sid parameter. **CVE ID : CVE-2020-13228**		060820/611
Session Fixation	02-06-2020	6.8	An issue was discovered in Sysax Multi Server 6.90. A session can be hijacked if one observes the sid value in any /scgi URI, because it is an authentication token. **CVE ID : CVE-2020-13229**	N/A	A-SYS-MULT-060820/612
targetcli-fb_project					
targetcli-fb					
Incorrect Default Permissions	05-06-2020	2.1	Open-iSCSI targetcli-fb through 2.1.52 has weak permissions for /etc/target (and for the backup directory and backup files). **CVE ID : CVE-2020-13867**	N/A	A-TAR-TARG-060820/613
the_rolling_proximity_identifier_project					
the_rolling_proximity_identifier					
Information Exposure	11-06-2020	6.4	** DISPUTED ** The Rolling Proximity Identifier used in the Apple/Google Exposure Notification API beta through 2020-05-29 enables attackers to circumvent Bluetooth Smart Privacy because there is a secondary temporary UID. An attacker with access to Beacon or IoT networks can seamlessly track individual device movement via a Bluetooth LE discovery mechanism.	N/A	A-THE-THE_-060820/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NOTE: this is disputed because the specification states "The advertiser address, Rolling Proximity Identifier, and Associated Encrypted Metadata shall be changed synchronously so that they cannot be linked" and therefore the purported tracking actually cannot occur. The original reporter says that synchronous changes only occur in one direction, not both directions. **CVE ID : CVE-2020-13702**		
themeboy					
sportspress					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	The SportsPress plugin before 2.7.2 for WordPress allows XSS. **CVE ID : CVE-2020-13892**	N/A	A-THE-SPOR-060820/615
Tibco					
managed_file_transfer_platform_server					
Missing Authorization	09-06-2020	9.3	The file transfer component of TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for IBM i contains a vulnerability that theoretically allows an attacker to perform unauthorized network file transfers to and from the file system accessible to the	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2020/06/tibco-security-	A-TIB-MANA-060820/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected component. This vulnerability is exploitable when the configuration option 'Require Node Resp' is set to 'No'. In the event of a successful exploit, the attacker could theoretically read and write any file on the file system accessible to the affected component, thus fully affecting the confidentiality, integrity, and availability of the operating system hosting the deployment of the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for IBM i: versions 7.1.0 and below, version 8.0.0. **CVE ID : CVE-2020-9411**	advisory-june-9-2020-tibco-managed-file-transfer-2020-9411	
Improper Input Validation	09-06-2020	10	The file transfer component of TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for IBM i contains a vulnerability that theoretically allows execution of arbitrary commands at the privilege level of the affected system following a failed file transfer. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for IBM i: versions 7.1.0 and below, version 8.0.0. **CVE ID : CVE-2020-9412**	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2020/06/tibco-security-advisory-june-9-2020-tibco-managed-file-transfer-2020-9412	A-TIB-MANA-060820/617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
treck					
tcp\/ip					
Authenticati on Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	A-TRE-TCP\-060820/618
Troglobit					
uftpd					
NULL Pointer Dereference	15-06-2020	5	In uftpd before 2.12, handle_CWD in ftpcmd.c mishandled the path provided by the user, causing a NULL pointer dereference and denial of service, as demonstrated by a CWD /.. command. **CVE ID : CVE-2020-14149**	N/A	A-TRO-UFTP-060820/619
ui					
unifi_controller					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network	N/A	A-UI-UNIF-060820/620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
url-regex_project					
url-regex					
Uncontrolled Resource Consumption	04-06-2020	7.8	all versions of url-regex are vulnerable to Regular Expression Denial of Service. An attacker providing a very long string in String.test can cause a Denial of Service. **CVE ID : CVE-2020-7661**	N/A	A-URL-URL--060820/621
verbb					
comments					
Cross-Site Request Forgery (CSRF)	05-06-2020	4.3	An issue was discovered in the Comments plugin before 1.5.5 for Craft CMS. CSRF affects comment integrity. **CVE ID : CVE-2020-13868**	N/A	A-VER-COMM-060820/622
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-06-2020	3.5	An issue was discovered in the Comments plugin before 1.5.6 for Craft CMS. There is stored XSS via a guest name. **CVE ID : CVE-2020-13869**	N/A	A-VER-COMM-060820/623
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-06-2020	3.5	An issue was discovered in the Comments plugin before 1.5.5 for Craft CMS. There is stored XSS via an asset volume name. **CVE ID : CVE-2020-13870**	N/A	A-VER-COMM-060820/624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Verizon					
serialize-javascript					
Deserialization of Untrusted Data	01-06-2020	6.8	serialize-javascript prior to 3.1.0 allows remote attackers to inject arbitrary code via the function "deleteFunctions" within "index.js". **CVE ID : CVE-2020-7660**	N/A	A-VER-SERI-060820/625
Videolan					
vlc_media_player					
Out-of-bounds Write	08-06-2020	6.8	A heap-based buffer overflow in the hxxx_AnnexB_to_xVC function in modules/packetizer/hxxx_nal.c in VideoLAN VLC media player before 3.0.11 for macOS/iOS allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a crafted H.264 Annex-B video (.avi for example) file. **CVE ID : CVE-2020-13428**	https://github.com/videolan/vlc-3.0/releases/tag/3.0.11, https://www.videolan.org/security/sb-vlc3011.html	A-VID-VLC_-060820/626
vm-memory_project					
vm-memory					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	5	rust-vmm vm-memory before 0.1.1 and 0.2.x before 0.2.1 allows attackers to cause a denial of service (loss of IP networking) because read_obj and write_obj do not properly access memory. This affects aarch64 (with musl or glibc) and x86_64 (with musl).	N/A	A-VM--VM-M-060820/627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13759		
Vmware					
spring_cloud_config					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-06-2020	5	Spring Cloud Config, versions 2.2.x prior to 2.2.3, versions 2.1.x prior to 2.1.9, and older unsupported versions allow applications to serve arbitrary configuration files through the spring-cloud-config-server module. A malicious user, or attacker, can send a request using a specially crafted URL that can lead to a directory traversal attack. **CVE ID : CVE-2020-5410**	https://tanzu.vmware.com/security/cve-2020-5410	A-VMW-SPRI-060820/628
horizon_client					
Improper Privilege Management	15-06-2020	4.6	VMware Horizon Client for Windows (prior to 5.4.3) contains a privilege escalation vulnerability due to folder permission configuration and unsafe loading of libraries. A local user on the system where the software is installed may exploit this issue to run commands as any user. **CVE ID : CVE-2020-3961**	N/A	A-VMW-HORI-060820/629
W1.fi					
hostapd					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL	N/A	A-W1.-HOST-060820/630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
weave					
weave_net					
Reliance on Reverse DNS Resolution for a Security-Critical Action	03-06-2020	3.5	In Weave Net before version 2.6.3, an attacker able to run a process as root in a container is able to respond to DNS requests from the host and thereby insert themselves as a fake service. In a cluster with an IPv4 internal network, if IPv6 is not totally disabled on the host (via ipv6.disable=1 on the kernel cmdline), it will be either unconfigured or configured on some interfaces, but it's pretty likely that ipv6 forwarding is disabled, ie /proc/sys/net/ipv6/conf//forwarding == 0. Also by default, /proc/sys/net/ipv6/conf//accept_ra == 1. The combination of these 2 sysctls means that the host accepts router advertisements and configure the IPv6 stack using them. By sending rogue router advertisements, an attacker can reconfigure the host to redirect part or all of the	https://github.com/weaveworks/weave/security/advisories/GHSA-59qg-grp7-5r73	A-WEA-WEAV-060820/631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPv6 traffic of the host to the attacker controlled container. Even if there was no IPv6 traffic before, if the DNS returns A (IPv4) and AAAA (IPv6) records, many HTTP libraries will try to connect via IPv6 first then fallback to IPv4, giving an opportunity to the attacker to respond. If by chance you also have on the host a vulnerability like last year's RCE in apt (CVE-2019-3462), you can now escalate to the host. Weave Net version 2.6.3 disables the accept_ra option on the veth devices that it creates. **CVE ID : CVE-2020-11091**		
Webroot					
endpoint_agents					
Access of Resource Using Incompatible Type ('Type Confusion')	15-06-2020	6.4	Webroot endpoint agents prior to version v9.0.28.48 allows remote attackers to trigger a type confusion vulnerability over its listening TCP port, resulting in crashing or reading memory contents of the Webroot endpoint agent. **CVE ID : CVE-2020-5754**	N/A	A-WEB-ENDP-060820/632
Improper Privilege Management	15-06-2020	6.9	Webroot endpoint agents prior to version v9.0.28.48 did not protect the "%PROGRAMDATA%\WrData\PKG" directory against renaming. This could allow attackers to trigger a crash	N/A	A-WEB-ENDP-060820/633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or wait upon Webroot service restart to rewrite and hijack dlls in this directory for privilege escalation. **CVE ID : CVE-2020-5755**		
websocket-extensions_project					
websocket-extensions					
N/A	02-06-2020	5	websocket-extensions npm module prior to 1.0.4 allows Denial of Service (DoS) via Regex Backtracking. The extension parser may take quadratic time when parsing a header containing an unclosed string parameter value whose content is a repeating two-byte sequence of a backslash and some other character. This could be abused by an attacker to conduct Regex Denial Of Service (ReDoS) on a single-threaded server by providing a malicious payload with the Sec-WebSocket-Extensions header. **CVE ID : CVE-2020-7662**	N/A	A-WEB-WEBS-060820/634
N/A	02-06-2020	5	websocket-extensions ruby module prior to 0.1.5 allows Denial of Service (DoS) via Regex Backtracking. The extension parser may take quadratic time when parsing a header containing an unclosed string parameter value whose content is a repeating two-byte sequence	N/A	A-WEB-WEBS-060820/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of a backslash and some other character. This could be abused by an attacker to conduct Regex Denial Of Service (ReDoS) on a single-threaded server by providing a malicious payload with the Sec-WebSocket-Extensions header. **CVE ID : CVE-2020-7663**		
whitesourcesoftware					
whitesource					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-06-2020	5	The dashboard in WhiteSource Application Vulnerability Management (AVM) before version 20.4.1 allows Log Injection via a %0A%0D substring in the idp parameter to the /saml/login URI. This closes the current log and creates a new log with one line of data. The attacker can also insert malicious data and false entries. **CVE ID : CVE-2020-5304**	N/A	A-WHI-WHIT-060820/636
Wordpress					
wordpress					
Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	12-06-2020	3.5	In affected versions of WordPress, users with low privileges (like contributors and authors) can use the embed block in a certain way to inject unfiltered HTML in the block editor. When affected posts are viewed by a higher privileged user, this could lead to script	https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-rpwf-hrh2-39jf	A-WOR-WORD-060820/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution in the editor/wp-admin. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34). **CVE ID : CVE-2020-4046**		
Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	12-06-2020	3.5	In affected versions of WordPress, authenticated users with upload permissions (like authors) are able to inject JavaScript into some media file attachment pages in a certain way. This can lead to script execution in the context of a higher privileged user when the file is viewed by them. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34). **CVE ID : CVE-2020-4047**	https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-8q2w-5m27-wm27	A-WOR-WORD-060820/638
URL Redirection to Untrusted Site ('Open Redirect')	12-06-2020	4.9	In affected versions of WordPress, due to an issue in wp_validate_redirect() and URL sanitization, an arbitrary external link can be crafted leading to unintended/open redirect when clicked. This has been	https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-q6pw-	A-WOR-WORD-060820/639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34). **CVE ID : CVE-2020-4048**	gvf4-5fj5	
Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	12-06-2020	3.5	In affected versions of WordPress, when uploading themes, the name of the theme folder can be crafted in a way that could lead to JavaScript execution in /wp-admin on the themes page. This does require an admin to upload the theme, and is low severity self-XSS. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34). **CVE ID : CVE-2020-4049**	https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-87h4-phjv-rm6p	A-WOR-WORD-060820/640
Authentication Bypass Using an Alternate Path or Channel	12-06-2020	6	In affected versions of WordPress, misuse of the `set-screen-option` filter's return value allows arbitrary user meta fields to be saved. It does require an admin to install a plugin that would misuse the filter. Once installed, it can be leveraged by low privileged users. This has been patched in version 5.4.2, along with all the	https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4vpv-fgg2-gcqc	A-WOR-WORD-060820/641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34). **CVE ID : CVE-2020-4050**		
Wso2					
api_microgateway					
Improper Restriction of XML External Entity Reference ('XXE')	06-06-2020	6.5	In WSO2 API Manager 3.0.0 and earlier, WSO2 API Microgateway 2.2.0, and WSO2 IS as Key Manager 5.9.0 and earlier, Management Console allows XXE during addition or update of a Lifecycle. **CVE ID : CVE-2020-13883**	N/A	A-WSO-API_-060820/642
identity_server_as_key_manager					
Improper Restriction of XML External Entity Reference ('XXE')	06-06-2020	6.5	In WSO2 API Manager 3.0.0 and earlier, WSO2 API Microgateway 2.2.0, and WSO2 IS as Key Manager 5.9.0 and earlier, Management Console allows XXE during addition or update of a Lifecycle. **CVE ID : CVE-2020-13883**	N/A	A-WSO-IDEN-060820/643
api_manager					
Improper Restriction of XML External Entity Reference ('XXE')	06-06-2020	6.5	In WSO2 API Manager 3.0.0 and earlier, WSO2 API Microgateway 2.2.0, and WSO2 IS as Key Manager 5.9.0 and earlier, Management Console allows XXE during addition or update of a Lifecycle.	N/A	A-WSO-API_-060820/644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13883		
xack					
xack_dns					
Uncontrolled Recursion	05-06-2020	5	XACK DNS 1.11.0 to 1.11.4, 1.10.0 to 1.10.8, 1.8.0 to 1.8.23, 1.7.0 to 1.7.18, and versions before 1.7.0 allow remote attackers to cause a denial of service condition resulting in degradation of the recursive resolver's performance or compromising the recursive resolver as a reflector in a reflection attack. **CVE ID : CVE-2020-5591**	N/A	A-XAC-XACK-060820/645
your_online_shop_project					
your_online_shop					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	3.5	Your Online Shop 1.8.0 allows authenticated users to trigger XSS via a Change Name or Change Surname operation. **CVE ID : CVE-2020-13911**	N/A	A-YOU-YOUR-060820/646
Zenphoto					
Zenphoto					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-06-2020	4.3	Cross-site scripting vulnerability in Zenphoto versions prior to 1.5.7 allows remote attackers to inject an arbitrary JavaScript via unspecified vectors. **CVE ID : CVE-2020-5592**	N/A	A-ZEN-ZENP-060820/647
Improper Neutralizatio	11-06-2020	6.5	Zenphoto versions prior to 1.5.7 allows an attacker to	N/A	A-ZEN-ZENP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements in Output Used by a Downstream Component ('Injection')			conduct PHP code injection attacks by leading a user to upload a specially crafted .zip file. **CVE ID : CVE-2020-5593**		060820/648
ZNC					
ZNC					
NULL Pointer Dereference	02-06-2020	3.5	ZNC 1.8.0 up to 1.8.1-rc1 allows authenticated users to trigger an application crash (with a NULL pointer dereference) if echo-message is not enabled and there is no network. **CVE ID : CVE-2020-13775**	https://github.com/znc/znc/commit/d229761821da38d984a9e4098ad96842490dc001	A-ZNC-ZNC-060820/649
Zohocorp					
manageengine_servicedesk_plus					
Missing Authentication for Critical Function	12-06-2020	5	Zoho ManageEngine ServiceDesk Plus before 11.1 build 11115 allows remote unauthenticated attackers to change the installation status of deployed agents. **CVE ID : CVE-2020-14048**	N/A	A-ZOH-MANA-060820/650
manageengine_opmanager					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-06-2020	5	In Zoho ManageEngine OpManager before 125144, when <cachestart> is used, directory traversal validation can be bypassed. **CVE ID : CVE-2020-13818**	N/A	A-ZOH-MANA-060820/651
Zoom					
zoom					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-06-2020	7.5	An exploitable path traversal vulnerability exists in the Zoom client, version 4.6.10 processes messages including animated GIFs. A specially crafted chat message can cause an arbitrary file write, which could potentially be abused to achieve arbitrary code execution. An attacker needs to send a specially crafted message to a target user or a group to exploit this vulnerability. **CVE ID : CVE-2020-6109**	N/A	A-ZOO-ZOOM-060820/652
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-06-2020	6.8	An exploitable partial path traversal vulnerability exists in the way Zoom Client version 4.6.10 processes messages including shared code snippets. A specially crafted chat message can cause an arbitrary binary planting which could be abused to achieve arbitrary code execution. An attacker needs to send a specially crafted message to a target user or a group to trigger this vulnerability. For the most severe effect, target user interaction is required. **CVE ID : CVE-2020-6110**	N/A	A-ZOO-ZOOM-060820/653
Operating System					
Apple					
mac_os					
Use After Free	03-06-2020	6.8	Use after free in payments in Google Chrome on MacOS	N/A	O-APP-MAC_-060820/654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 83.0.4103.97 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2020-6496**		
Use After Free	12-06-2020	10	Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9633**	https://helpx.adobe.com/security/products/flash-player/apsb20-30.html	O-APP-MAC_-060820/655
iphone_os					
Incorrect Default Permissions	03-06-2020	4.3	Insufficient policy enforcement in Omnibox in Google Chrome on iOS prior to 83.0.4103.88 allowed a remote attacker to perform domain spoofing via a crafted URI. **CVE ID : CVE-2020-6497**	N/A	O-APP-IPHO-060820/656
Incorrect Default Permissions	03-06-2020	4.3	Incorrect implementation in user interface in Google Chrome on iOS prior to 83.0.4103.88 allowed a remote attacker to perform domain spoofing via a crafted HTML page. **CVE ID : CVE-2020-6498**	N/A	O-APP-IPHO-060820/657
Out-of-bounds	09-06-2020	9.3	An out-of-bounds write issue was addressed with	N/A	O-APP-IPHO-060820/658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9789**		
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9790**	N/A	O-APP-IPHO-060820/659
Out-of-bounds Read	09-06-2020	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9791**	N/A	O-APP-IPHO-060820/660
Improper Input	09-06-2020	2.1	A validation issue was addressed with improved	N/A	O-APP-IPHO-060820/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			input sanitization. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A USB device may be able to cause a denial of service. **CVE ID : CVE-2020-9792**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-9793**	N/A	O-APP-IPHO-060820/662
Out-of-bounds Read	09-06-2020	5.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A malicious application may cause a denial of service or potentially disclose memory contents. **CVE ID : CVE-2020-9794**	N/A	O-APP-IPHO-060820/663
Use After Free	09-06-2020	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5,	N/A	O-APP-IPHO-060820/664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 6.2.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9795**		
Information Exposure	09-06-2020	4.3	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to determine another application's memory layout. **CVE ID : CVE-2020-9797**	N/A	O-APP-IPHO-060820/665
Access of Resource Using Incompatible Type ('Type Confusion')	09-06-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9800**	N/A	O-APP-IPHO-060820/666
N/A	09-06-2020	6.8	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously	N/A	O-APP-IPHO-060820/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9802**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9803**	N/A	O-APP-IPHO-060820/668
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9805**	N/A	O-APP-IPHO-060820/669
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud	N/A	O-APP-IPHO-060820/670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9806**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9807**	N/A	O-APP-IPHO-060820/671
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	5.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2020-9808**	N/A	O-APP-IPHO-060820/672
Information Exposure	09-06-2020	7.1	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina	N/A	O-APP-IPHO-060820/673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9809**		
Information Exposure	09-06-2020	4.3	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9811**	N/A	O-APP-IPHO-060820/674
Information Exposure	09-06-2020	7.1	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9812**	N/A	O-APP-IPHO-060820/675
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with	N/A	O-APP-IPHO-060820/676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel privileges. **CVE ID : CVE-2020-9813**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9814**	N/A	O-APP-IPHO-060820/677
Out-of-bounds Read	09-06-2020	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9815**	N/A	O-APP-IPHO-060820/678
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9816**	N/A	O-APP-IPHO-060820/679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	09-06-2020	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, iOS 12.4.7, watchOS 6.2.5. Processing a maliciously crafted mail message may lead to unexpected memory modification or application termination. **CVE ID : CVE-2020-9818**	N/A	O-APP-IPHO-060820/680
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	4.3	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, iOS 12.4.7, watchOS 6.2.5, watchOS 5.3.7. Processing a maliciously crafted mail message may lead to heap corruption. **CVE ID : CVE-2020-9819**	N/A	O-APP-IPHO-060820/681
N/A	09-06-2020	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5. A remote attacker may be able to modify the file system. **CVE ID : CVE-2020-9820**	N/A	O-APP-IPHO-060820/682
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to	N/A	O-APP-IPHO-060820/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9821**		
N/A	09-06-2020	5	This issue was addressed with improved checks. This issue is fixed in iOS 13.5 and iPadOS 13.5. Users removed from an iMessage conversation may still be able to alter state. **CVE ID : CVE-2020-9823**	N/A	O-APP-IPHO-060820/684
N/A	09-06-2020	6.8	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A malicious application may be able to bypass Privacy preferences. **CVE ID : CVE-2020-9825**	N/A	O-APP-IPHO-060820/685
Improper Input Validation	09-06-2020	5	A denial of service issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9826**	N/A	O-APP-IPHO-060820/686
N/A	09-06-2020	5	A denial of service issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A remote attacker may be able to cause a denial of service.	N/A	O-APP-IPHO-060820/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9827		
Improper Input Validation	09-06-2020	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted text message may lead to application denial of service. **CVE ID : CVE-2020-9829**	N/A	O-APP-IPHO-060820/688
Improper Input Validation	09-06-2020	5	An issue existed in the pausing of FaceTime video. The issue was resolved with improved logic. This issue is fixed in iOS 13.5 and iPadOS 13.5. A user's video may not be paused in a FaceTime call if they exit the FaceTime app while the call is ringing. **CVE ID : CVE-2020-9835**	N/A	O-APP-IPHO-060820/689
Out-of-bounds Read	09-06-2020	5	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5. A remote attacker may be able to leak memory. **CVE ID : CVE-2020-9837**	N/A	O-APP-IPHO-060820/690
Out-of-bounds Read	09-06-2020	7.5	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5. A remote attacker may be able to cause arbitrary code execution.	N/A	O-APP-IPHO-060820/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9838		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-06-2020	5.1	A race condition was addressed with improved state handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to gain elevated privileges. **CVE ID : CVE-2020-9839**	N/A	O-APP-IPHO-060820/692
N/A	09-06-2020	4.3	This issue was addressed with improved checks. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to use arbitrary entitlements. **CVE ID : CVE-2020-9842**	N/A	O-APP-IPHO-060820/693
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9843**	N/A	O-APP-IPHO-060820/694
Double Free	09-06-2020	7.8	A double free issue was addressed with improved memory management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina	N/A	O-APP-IPHO-060820/695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.15.5. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2020-9844**		
Information Exposure	09-06-2020	2.1	An authorization issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5. A person with physical access to an iOS device may be able to view notification contents from the lockscreen. **CVE ID : CVE-2020-9848**	N/A	O-APP-IPHO-060820/696
N/A	09-06-2020	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-9850**	N/A	O-APP-IPHO-060820/697
Integer Overflow or Wraparound	09-06-2020	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9852**	N/A	O-APP-IPHO-060820/698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	05-06-2020	7.2	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5.1 and iPadOS 13.5.1, macOS Catalina 10.15.5 Supplemental Update, tvOS 13.4.6, watchOS 6.2.6. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9859**	N/A	O-APP-IPHO-060820/699
mac_os_x					
Information Exposure	09-06-2020	4.3	This issue was addressed with improved checks. This issue is fixed in macOS Catalina 10.15.5. Importing a maliciously crafted calendar invitation may exfiltrate user information. **CVE ID : CVE-2020-3882**	N/A	O-APP-MAC_-060820/700
Improper Input Validation	09-06-2020	9.3	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Catalina 10.15.5. A file may be incorrectly rendered to execute JavaScript. **CVE ID : CVE-2020-9788**	N/A	O-APP-MAC_-060820/701
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a	N/A	O-APP-MAC_-060820/702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9789**		
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9790**	N/A	O-APP-MAC_-060820/703
Out-of-bounds Read	09-06-2020	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9791**	N/A	O-APP-MAC_-060820/704
Improper Input Validation	09-06-2020	2.1	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A USB device may be able to cause a denial of service. **CVE ID : CVE-2020-9792**	N/A	O-APP-MAC_-060820/705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-9793**	N/A	O-APP-MAC_-060820/706
Out-of-bounds Read	09-06-2020	5.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A malicious application may cause a denial of service or potentially disclose memory contents. **CVE ID : CVE-2020-9794**	N/A	O-APP-MAC_-060820/707
Use After Free	09-06-2020	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9795**	N/A	O-APP-MAC_-060820/708
Information Exposure	09-06-2020	4.3	An information disclosure issue was addressed by	N/A	O-APP-MAC_-060820/709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			removing the vulnerable code. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to determine another application's memory layout. **CVE ID : CVE-2020-9797**		
Access of Resource Using Incompatible Type ('Type Confusion')	09-06-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9800**	N/A	O-APP-MAC_-060820/710
N/A	09-06-2020	4.9	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.5. Inserting a USB device that sends invalid messages may cause a kernel panic. **CVE ID : CVE-2020-9804**	N/A	O-APP-MAC_-060820/711
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	5.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An	N/A	O-APP-MAC_-060820/712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2020-9808**		
Information Exposure	09-06-2020	7.1	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9809**	N/A	O-APP-MAC_-060820/713
Information Exposure	09-06-2020	4.3	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9811**	N/A	O-APP-MAC_-060820/714
Information Exposure	09-06-2020	7.1	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9812**	N/A	O-APP-MAC_-060820/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9813**	N/A	O-APP-MAC_-060820/716
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9814**	N/A	O-APP-MAC_-060820/717
Out-of-bounds Read	09-06-2020	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9815**	N/A	O-APP-MAC_-060820/718
Out-of-bounds	09-06-2020	9.3	An out-of-bounds write issue was addressed with	N/A	O-APP-MAC_-060820/719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9816**		
Incorrect Default Permissions	09-06-2020	9.3	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in macOS Catalina 10.15.5. A malicious application may be able to gain root privileges. **CVE ID : CVE-2020-9817**	N/A	O-APP-MAC_-060820/720
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9821**	N/A	O-APP-MAC_-060820/721
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9822**	N/A	O-APP-MAC_-060820/722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.5. A non-privileged user may be able to modify restricted network settings. **CVE ID : CVE-2020-9824**	N/A	O-APP-MAC_-060820/723
N/A	09-06-2020	6.8	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A malicious application may be able to bypass Privacy preferences. **CVE ID : CVE-2020-9825**	N/A	O-APP-MAC_-060820/724
Improper Input Validation	09-06-2020	5	A denial of service issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9826**	N/A	O-APP-MAC_-060820/725
N/A	09-06-2020	5	A denial of service issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9827**	N/A	O-APP-MAC_-060820/726
Improper Restriction of	09-06-2020	9.3	A memory corruption issue was addressed with improved state	N/A	O-APP-MAC_-060820/727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			management. This issue is fixed in macOS Catalina 10.15.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9830**		
Out-of-bounds Read	09-06-2020	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.5. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9831**	N/A	O-APP-MAC_-060820/728
Out-of-bounds Read	09-06-2020	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.5. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9832**	N/A	O-APP-MAC_-060820/729
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	4.9	A memory initialization issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.5. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9833**	N/A	O-APP-MAC_-060820/730
Improper Restriction of Operations within the Bounds of a Memory	09-06-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.5. An application may be able to execute arbitrary code with	N/A	O-APP-MAC_-060820/731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			kernel privileges. **CVE ID : CVE-2020-9834**		
Out-of-bounds Read	09-06-2020	5	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5. A remote attacker may be able to leak memory. **CVE ID : CVE-2020-9837**	N/A	O-APP-MAC_-060820/732
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-06-2020	5.1	A race condition was addressed with improved state handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to gain elevated privileges. **CVE ID : CVE-2020-9839**	N/A	O-APP-MAC_-060820/733
Integer Overflow or Wraparound	09-06-2020	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Catalina 10.15.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9841**	N/A	O-APP-MAC_-060820/734
N/A	09-06-2020	4.3	This issue was addressed with improved checks. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to use arbitrary entitlements. **CVE ID : CVE-2020-9842**	N/A	O-APP-MAC_-060820/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	09-06-2020	7.8	A double free issue was addressed with improved memory management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2020-9844**	N/A	O-APP-MAC_-060820/736
Out-of-bounds Read	09-06-2020	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.5. A malicious application may be able to break out of its sandbox. **CVE ID : CVE-2020-9847**	N/A	O-APP-MAC_-060820/737
Incorrect Permission Assignment for Critical Resource	09-06-2020	4.3	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Catalina 10.15.5. A malicious application may be able to modify protected parts of the file system. **CVE ID : CVE-2020-9851**	N/A	O-APP-MAC_-060820/738
Integer Overflow or Wraparound	09-06-2020	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9852**	N/A	O-APP-MAC_-060820/739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-06-2020	4.6	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Catalina 10.15.5. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-9855**	N/A	O-APP-MAC_-060820/740
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	4.6	This issue was addressed with improved checks. This issue is fixed in macOS Catalina 10.15.5. An application may be able to gain elevated privileges. **CVE ID : CVE-2020-9856**	N/A	O-APP-MAC_-060820/741
Uncontrolled Resource Consumption	05-06-2020	7.2	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5.1 and iPadOS 13.5.1, macOS Catalina 10.15.5 Supplemental Update, tvOS 13.4.6, watchOS 6.2.6. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9859**	N/A	O-APP-MAC_-060820/742
watchos					
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for	N/A	O-APP-WATC-060820/743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9789**		
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9790**	N/A	O-APP-WATC-060820/744
Out-of-bounds Read	09-06-2020	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9791**	N/A	O-APP-WATC-060820/745
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A remote attacker may be able to cause arbitrary code	N/A	O-APP-WATC-060820/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-9793**		
Out-of-bounds Read	09-06-2020	5.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A malicious application may cause a denial of service or potentially disclose memory contents. **CVE ID : CVE-2020-9794**	N/A	O-APP-WATC-060820/747
Use After Free	09-06-2020	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9795**	N/A	O-APP-WATC-060820/748
Information Exposure	09-06-2020	4.3	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to determine another application's memory layout. **CVE ID : CVE-2020-9797**	N/A	O-APP-WATC-060820/749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	09-06-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9800**	N/A	O-APP-WATC-060820/750
N/A	09-06-2020	6.8	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9802**	N/A	O-APP-WATC-060820/751
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	O-APP-WATC-060820/752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9803		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9805**	N/A	O-APP-WATC-060820/753
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9806**	N/A	O-APP-WATC-060820/754
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to	N/A	O-APP-WATC-060820/755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-9807**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	5.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2020-9808**	N/A	O-APP-WATC-060820/756
Information Exposure	09-06-2020	7.1	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9809**	N/A	O-APP-WATC-060820/757
Information Exposure	09-06-2020	4.3	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9811**	N/A	O-APP-WATC-060820/758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	09-06-2020	7.1	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9812**	N/A	O-APP-WATC-060820/759
Out-of-bounds Read	09-06-2020	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9815**	N/A	O-APP-WATC-060820/760
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9816**	N/A	O-APP-WATC-060820/761
Out-of-bounds Write	09-06-2020	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, iOS 12.4.7,	N/A	O-APP-WATC-060820/762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 6.2.5. Processing a maliciously crafted mail message may lead to unexpected memory modification or application termination. **CVE ID : CVE-2020-9818**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	4.3	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, iOS 12.4.7, watchOS 6.2.5, watchOS 5.3.7. Processing a maliciously crafted mail message may lead to heap corruption. **CVE ID : CVE-2020-9819**	N/A	O-APP-WATC-060820/763
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9821**	N/A	O-APP-WATC-060820/764
N/A	09-06-2020	5	A denial of service issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A remote attacker may be able to cause a denial of service.	N/A	O-APP-WATC-060820/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9827		
Improper Input Validation	09-06-2020	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted text message may lead to application denial of service. **CVE ID : CVE-2020-9829**	N/A	O-APP-WATC-060820/766
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-06-2020	5.1	A race condition was addressed with improved state handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to gain elevated privileges. **CVE ID : CVE-2020-9839**	N/A	O-APP-WATC-060820/767
N/A	09-06-2020	4.3	This issue was addressed with improved checks. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to use arbitrary entitlements. **CVE ID : CVE-2020-9842**	N/A	O-APP-WATC-060820/768
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19.	N/A	O-APP-WATC-060820/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9843**		
N/A	09-06-2020	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-9850**	N/A	O-APP-WATC-060820/770
Integer Overflow or Wraparound	09-06-2020	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9852**	N/A	O-APP-WATC-060820/771
Uncontrolled Resource Consumption	05-06-2020	7.2	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5.1 and iPadOS 13.5.1, macOS Catalina 10.15.5 Supplemental Update, tvOS 13.4.6, watchOS 6.2.6. An application may be able to execute arbitrary code with kernel privileges.	N/A	O-APP-WATC-060820/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9859		
tvos					
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9789**	N/A	O-APP-TVOS-060820/773
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9790**	N/A	O-APP-TVOS-060820/774
Out-of-bounds Read	09-06-2020	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted audio file may lead to arbitrary code	N/A	O-APP-TVOS-060820/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-9791**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-9793**	N/A	O-APP-TVOS-060820/776
Out-of-bounds Read	09-06-2020	5.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A malicious application may cause a denial of service or potentially disclose memory contents. **CVE ID : CVE-2020-9794**	N/A	O-APP-TVOS-060820/777
Use After Free	09-06-2020	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9795**	N/A	O-APP-TVOS-060820/778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	09-06-2020	4.3	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to determine another application's memory layout. **CVE ID : CVE-2020-9797**	N/A	O-APP-TVOS-060820/779
N/A	09-06-2020	6.8	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9802**	N/A	O-APP-TVOS-060820/780
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9803**	N/A	O-APP-TVOS-060820/781
Improper	09-06-2020	4.3	A logic issue was addressed	N/A	O-APP-TVOS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9805**		060820/782
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9806**	N/A	O-APP-TVOS-060820/783
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	O-APP-TVOS-060820/784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9807		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	5.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2020-9808**	N/A	O-APP-TVOS-060820/785
Information Exposure	09-06-2020	7.1	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9809**	N/A	O-APP-TVOS-060820/786
Information Exposure	09-06-2020	4.3	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9811**	N/A	O-APP-TVOS-060820/787
Information Exposure	09-06-2020	7.1	An information disclosure issue was addressed with	N/A	O-APP-TVOS-060820/788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9812**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9813**	N/A	O-APP-TVOS-060820/789
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9814**	N/A	O-APP-TVOS-060820/790
Out-of-bounds Read	09-06-2020	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and	N/A	O-APP-TVOS-060820/791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9815**		
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9816**	N/A	O-APP-TVOS-060820/792
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9821**	N/A	O-APP-TVOS-060820/793
N/A	09-06-2020	5	A denial of service issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A remote attacker may be able to	N/A	O-APP-TVOS-060820/794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service. **CVE ID : CVE-2020-9827**		
Improper Input Validation	09-06-2020	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted text message may lead to application denial of service. **CVE ID : CVE-2020-9829**	N/A	O-APP-TVOS-060820/795
Out-of-bounds Read	09-06-2020	5	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5. A remote attacker may be able to leak memory. **CVE ID : CVE-2020-9837**	N/A	O-APP-TVOS-060820/796
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-06-2020	5.1	A race condition was addressed with improved state handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to gain elevated privileges. **CVE ID : CVE-2020-9839**	N/A	O-APP-TVOS-060820/797
N/A	09-06-2020	4.3	This issue was addressed with improved checks. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to	N/A	O-APP-TVOS-060820/798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use arbitrary entitlements. **CVE ID : CVE-2020-9842**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-06-2020	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9843**	N/A	O-APP-TVOS-060820/799
N/A	09-06-2020	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-9850**	N/A	O-APP-TVOS-060820/800
Integer Overflow or Wraparound	09-06-2020	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9852**	N/A	O-APP-TVOS-060820/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	05-06-2020	7.2	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5.1 and iPadOS 13.5.1, macOS Catalina 10.15.5 Supplemental Update, tvOS 13.4.6, watchOS 6.2.6. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9859**	N/A	O-APP-TVOS-060820/802
ipados					
Use After Free	09-06-2020	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9795**	N/A	O-APP-IPAD-060820/803
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9803**	N/A	O-APP-IPAD-060820/804
Improper	09-06-2020	6.8	A memory corruption issue	N/A	O-APP-IPAD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9806**		060820/805
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9807**	N/A	O-APP-IPAD-060820/806
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	5.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to cause unexpected system termination or write kernel memory.	N/A	O-APP-IPAD-060820/807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9808		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9813**	N/A	O-APP-IPAD-060820/808
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9814**	N/A	O-APP-IPAD-060820/809
Out-of-bounds Read	09-06-2020	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9815**	N/A	O-APP-IPAD-060820/810
Out-of-	09-06-2020	6.8	An out-of-bounds write issue	N/A	O-APP-IPAD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, iOS 12.4.7, watchOS 6.2.5. Processing a maliciously crafted mail message may lead to unexpected memory modification or application termination. **CVE ID : CVE-2020-9818**		060820/811
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	4.3	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, iOS 12.4.7, watchOS 6.2.5, watchOS 5.3.7. Processing a maliciously crafted mail message may lead to heap corruption. **CVE ID : CVE-2020-9819**	N/A	O-APP-IPAD-060820/812
N/A	09-06-2020	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5. A remote attacker may be able to modify the file system. **CVE ID : CVE-2020-9820**	N/A	O-APP-IPAD-060820/813
N/A	09-06-2020	6.8	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A malicious application may be able to bypass Privacy preferences. **CVE ID : CVE-2020-9825**	N/A	O-APP-IPAD-060820/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipad_os					
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9789**	N/A	O-APP-IPAD-060820/815
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9790**	N/A	O-APP-IPAD-060820/816
Out-of-bounds Read	09-06-2020	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted audio file may lead to arbitrary code execution.	N/A	O-APP-IPAD-060820/817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9791		
Improper Input Validation	09-06-2020	2.1	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A USB device may be able to cause a denial of service. **CVE ID : CVE-2020-9792**	N/A	O-APP-IPAD-060820/818
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-9793**	N/A	O-APP-IPAD-060820/819
Out-of-bounds Read	09-06-2020	5.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A malicious application may cause a denial of service or potentially disclose memory contents. **CVE ID : CVE-2020-9794**	N/A	O-APP-IPAD-060820/820
Information Exposure	09-06-2020	4.3	An information disclosure issue was addressed by removing the vulnerable	N/A	O-APP-IPAD-060820/821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to determine another application's memory layout. **CVE ID : CVE-2020-9797**		
Access of Resource Using Incompatible Type ('Type Confusion')	09-06-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9800**	N/A	O-APP-IPAD-060820/822
N/A	09-06-2020	6.8	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9802**	N/A	O-APP-IPAD-060820/823
Improper Neutralization of Input During Web	09-06-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5,	N/A	O-APP-IPAD-060820/824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9805**		
Information Exposure	09-06-2020	7.1	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9809**	N/A	O-APP-IPAD-060820/825
Information Exposure	09-06-2020	4.3	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9811**	N/A	O-APP-IPAD-060820/826
Information Exposure	09-06-2020	7.1	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5,	N/A	O-APP-IPAD-060820/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 6.2.5. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9812**		
Out-of-bounds Write	09-06-2020	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9816**	N/A	O-APP-IPAD-060820/828
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9821**	N/A	O-APP-IPAD-060820/829
N/A	09-06-2020	5	This issue was addressed with improved checks. This issue is fixed in iOS 13.5 and iPadOS 13.5. Users removed from an iMessage conversation may still be able to alter state. **CVE ID : CVE-2020-9823**	N/A	O-APP-IPAD-060820/830
Improper Input	09-06-2020	5	A denial of service issue was addressed with improved input validation. This issue is	N/A	O-APP-IPAD-060820/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9826**		
N/A	09-06-2020	5	A denial of service issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9827**	N/A	O-APP-IPAD-060820/832
Improper Input Validation	09-06-2020	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5. Processing a maliciously crafted text message may lead to application denial of service. **CVE ID : CVE-2020-9829**	N/A	O-APP-IPAD-060820/833
Improper Input Validation	09-06-2020	5	An issue existed in the pausing of FaceTime video. The issue was resolved with improved logic. This issue is fixed in iOS 13.5 and iPadOS 13.5. A user's video may not be paused in a FaceTime call if they exit the FaceTime app while the call is ringing. **CVE ID : CVE-2020-9835**	N/A	O-APP-IPAD-060820/834
Out-of-bounds Read	09-06-2020	5	An out-of-bounds read was addressed with improved bounds checking. This issue	N/A	O-APP-IPAD-060820/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5. A remote attacker may be able to leak memory. **CVE ID : CVE-2020-9837**		
Out-of-bounds Read	09-06-2020	7.5	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-9838**	N/A	O-APP-IPAD-060820/836
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-06-2020	5.1	A race condition was addressed with improved state handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to gain elevated privileges. **CVE ID : CVE-2020-9839**	N/A	O-APP-IPAD-060820/837
N/A	09-06-2020	4.3	This issue was addressed with improved checks. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. An application may be able to use arbitrary entitlements. **CVE ID : CVE-2020-9842**	N/A	O-APP-IPAD-060820/838
Improper Neutralization of Input During Web Page	09-06-2020	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5,	N/A	O-APP-IPAD-060820/839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9843**		
Double Free	09-06-2020	7.8	A double free issue was addressed with improved memory management. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2020-9844**	N/A	O-APP-IPAD-060820/840
Information Exposure	09-06-2020	2.1	An authorization issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5. A person with physical access to an iOS device may be able to view notification contents from the lockscreen. **CVE ID : CVE-2020-9848**	N/A	O-APP-IPAD-060820/841
N/A	09-06-2020	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A remote attacker may be able	N/A	O-APP-IPAD-060820/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to cause arbitrary code execution. **CVE ID : CVE-2020-9850**		
Integer Overflow or Wraparound	09-06-2020	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9852**	N/A	O-APP-IPAD-060820/843
Uncontrolled Resource Consumption	05-06-2020	7.2	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5.1 and iPadOS 13.5.1, macOS Catalina 10.15.5 Supplemental Update, tvOS 13.4.6, watchOS 6.2.6. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9859**	N/A	O-APP-IPAD-060820/844
ARM					
cortex-a57_firmware					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation."	http://lists.llvm.org/pipermail/llvm-dev/2020-June/142109.html, https://developer.arm.com/support/arm-security-	O-ARM-CORT-060820/845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13844	updates/speculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/547520.html	
cortex-a72_firmware					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	http://lists.llvm.org/pipermail/llvm-dev/2020-June/142109.html, https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/547520.html	O-ARM-CORT-060820/846
cortex-a73_firmware					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past	http://lists.llvm.org/pipermail/llvm	O-ARM-CORT-060820/847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	-dev/2020-June/142109.html, https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/547520.html	
cortex-a34_firmware					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	http://lists.llvm.org/pipermail/llvm-dev/2020-June/142109.html, https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/20	O-ARM-CORT-060820/848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				20-June/547520.html	
cortex-a32_firmware					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	http://lists.llvm.org/pipermail/llvm-dev/2020-June/142109.html, https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/547520.html	O-ARM-CORT-060820/849
cortex-a35_firmware					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	http://lists.llvm.org/pipermail/llvm-dev/2020-June/142109.html, https://developer.arm.com/support/arm-security-updates/sp	O-ARM-CORT-060820/850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				eculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/547520.html	
cortex-a53_firmware					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	http://lists.llvm.org/pipermail/llvm-dev/2020-June/142109.html, https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/547520.html	O-ARM-CORT-060820/851
Canonical					
ubuntu_linux					
Use of a Broken or Risky	04-06-2020	5.8	GnuTLS 3.6.x before 3.6.14 uses incorrect cryptography for encrypting a session	https://gnutls.org/security-	O-CAN-UBUN-060820/852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Algorithm			ticket (a loss of confidentiality in TLS 1.2, and an authentication bypass in TLS 1.3). The earliest affected version is 3.6.4 (2018-09-24) because of an error in a 2018-09-18 commit. Until the first key rotation, the TLS server always uses wrong data in place of an encryption key derived from an application. **CVE ID : CVE-2020-13777**	new.html#GNUTLS-SA-2020-06-03, https://security.netapp.com/advisory/ntap-20200619-0004/	
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	O-CAN-UBUN-060820/853
Improper Certificate Validation	03-06-2020	4.3	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. In cases where a memcached backend does not perform key validation, passing malformed cache keys could result in a key collision, and potential data leakage. **CVE ID : CVE-2020-13254**	https://security.netapp.com/advisory/ntap-20200611-0002/, https://www.djangoproject.com/weblog/2020/jun/03/security-releases/	O-CAN-UBUN-060820/854
castel					
nextgen_dvr_firmware					
Improper Privilege	04-06-2020	6.5	Castel NextGen DVR v1.0.0 is vulnerable to privilege	N/A	O-CAS-NEXT-060820/855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			escalation through the Adminstrator/Users/Edit/:UserId functionality. Adminstrator/Users/Edit/:UserId fails to check that the request was submitted by an Administrator. This allows a normal user to escalate their privileges by adding additional roles to their account. **CVE ID : CVE-2020-11679**		
Incorrect Authorization	04-06-2020	4	Castel NextGen DVR v1.0.0 is vulnerable to authorization bypass on all administrator functionality. The application fails to check that a request was submitted by an administrator. Consequently, a normal user can perform actions including, but not limited to, creating/modifying the file store, creating/modifying alerts, creating/modifying users, etc. **CVE ID : CVE-2020-11680**	N/A	O-CAS-NEXT-060820/856
Insufficiently Protected Credentials	04-06-2020	4	Castel NextGen DVR v1.0.0 stores and displays credentials for the associated SMTP server in cleartext. Low privileged users can exploit this to create an administrator user and obtain the SMTP credentials. **CVE ID : CVE-2020-11681**	N/A	O-CAS-NEXT-060820/857
Cross-Site Request	04-06-2020	4.3	Castel NextGen DVR v1.0.0 is vulnerable to CSRF in all	N/A	O-CAS-NEXT-060820/858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			state-changing request. A __RequestVerificationToken is set by the web interface, and included in requests sent by web interface. However, this token is not verified by the application: the token can be removed from all requests and the request will succeed. **CVE ID : CVE-2020-11682**		
Cisco					
nx-os					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the	N/A	O-CIS-NX-O-060820/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
Authenticati on Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	O-CIS-NX-O-060820/860
ios_xr					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length	N/A	O-CIS-IOS_-060820/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
ios					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3198**	N/A	O-CIS-IOS-060820/862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	03-06-2020	8.3	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3199**	N/A	O-CIS-IOS-060820/863
Interpretation Conflict	03-06-2020	6.8	A vulnerability in the Secure Shell (SSH) server code of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload. The vulnerability is due to an internal state not being represented correctly in the SSH state machine, which leads to an unexpected behavior. An attacker could exploit this vulnerability by creating an SSH connection to an affected device and using a specific traffic pattern that causes an error condition within that connection. A successful exploit could allow an	N/A	O-CIS-IOS-060820/864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause the device to reload, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2020-3200**		
Improper Input Validation	03-06-2020	4.9	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker with privileged EXEC credentials to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by executing crafted Tcl arguments on an affected device. An exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3201**	N/A	O-CIS-IOS-060820/865
Improper Input Validation	03-06-2020	7.2	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker with privileged EXEC credentials to execute arbitrary code on the underlying operating system (OS) with root privileges. The vulnerability is due to	N/A	O-CIS-IOS-060820/866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by loading malicious Tcl code on an affected device. A successful exploit could allow the attacker to cause memory corruption or execute the code with root privileges on the underlying OS of the affected device. **CVE ID : CVE-2020-3204**		
Improper Input Validation	03-06-2020	8.3	A vulnerability in the implementation of the inter-VM channel of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, adjacent attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The vulnerability is due to insufficient validation of signaling packets that are destined to VDS. An attacker could exploit this vulnerability by sending malicious packets to an affected device. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root	N/A	O-CIS-IOS-060820/867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user. Because the device is designed on a hypervisor architecture, exploitation of a vulnerability that affects the inter-VM channel may lead to a complete system compromise. For more information about this vulnerability, see the Details section of this advisory. **CVE ID : CVE-2020-3205**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in the image verification feature of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) could allow an authenticated, local attacker to boot a malicious software image on an affected device. The vulnerability is due to insufficient access restrictions on the area of code that manages the image verification feature. An attacker could exploit this vulnerability by first authenticating to the targeted device and then logging in to the Virtual Device Server (VDS) of an affected device. The attacker could then, from the VDS shell, disable Cisco IOS Software integrity (image) verification. A successful exploit could allow the attacker to boot a malicious Cisco IOS Software image on the targeted device. To	N/A	O-CIS-IOS-060820/868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability, the attacker must have valid user credentials at privilege level 15. **CVE ID : CVE-2020-3208**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the CLI parsers of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated, local attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The attacker must have valid user credentials at privilege level 15. The vulnerability is due to insufficient validation of arguments that are passed to specific VDS-related CLI commands. An attacker could exploit this vulnerability by authenticating to the targeted device and including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. **CVE ID : CVE-2020-3210**	N/A	O-CIS-IOS-060820/869
Improper	03-06-2020	8.3	A vulnerability in the	N/A	O-CIS-IOS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		060820/870
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid	N/A	O-CIS-IOS-060820/871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	O-CIS-IOS-060820/872
Improper Input Validation	03-06-2020	7.8	Multiple vulnerabilities in the implementation of the Common Industrial Protocol (CIP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected	N/A	O-CIS-IOS-060820/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to insufficient input processing of CIP traffic. An attacker could exploit these vulnerabilities by sending crafted CIP traffic to be processed by an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3225**		
Improper Input Validation	03-06-2020	7.8	A vulnerability in the Session Initiation Protocol (SIP) library of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient sanity checks on received SIP messages. An attacker could exploit this vulnerability by sending crafted SIP messages to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service condition. **CVE ID : CVE-2020-3226**	N/A	O-CIS-IOS-060820/874
Improper	03-06-2020	7.8	A vulnerability in Security	N/A	O-CIS-IOS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Group Tag Exchange Protocol (SXP) in Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because crafted SXP packets are mishandled. An attacker could exploit this vulnerability by sending specifically crafted SXP packets to the affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3228**		060820/875
Improper Input Validation	03-06-2020	5	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to prevent IKEv2 from establishing new security associations. The vulnerability is due to incorrect handling of crafted IKEv2 SA-Init packets. An attacker could exploit this vulnerability by sending crafted IKEv2 SA-Init packets to the affected device. An exploit could	N/A	O-CIS-IOS-060820/876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the affected device to reach the maximum incoming negotiation limits and prevent further IKEv2 security associations from being formed. **CVE ID : CVE-2020-3230**		
Incorrect Authorization	03-06-2020	2.9	A vulnerability in the 802.1X feature of Cisco Catalyst 2960-L Series Switches and Cisco Catalyst CDB-8P Switches could allow an unauthenticated, adjacent attacker to forward broadcast traffic before being authenticated on the port. The vulnerability exists because broadcast traffic that is received on the 802.1X-enabled port is mishandled. An attacker could exploit this vulnerability by sending broadcast traffic on the port before being authenticated. A successful exploit could allow the attacker to send and receive broadcast traffic on the 802.1X-enabled port before authentication. **CVE ID : CVE-2020-3231**	N/A	O-CIS-IOS-060820/877
Use of Hard-coded Credentials	03-06-2020	7.2	A vulnerability in the virtual console authentication of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could	N/A	O-CIS-IOS-060820/878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated but low-privileged, local attacker to log in to the Virtual Device Server (VDS) of an affected device by using a set of default credentials. The vulnerability is due to the presence of weak, hard-coded credentials. An attacker could exploit this vulnerability by authenticating to the targeted device and then connecting to VDS through the device’s virtual console by using the static credentials. A successful exploit could allow the attacker to access the Linux shell of VDS as the root user. **CVE ID : CVE-2020-3234**		
Improper Input Validation	03-06-2020	6.3	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software on Catalyst 4500 Series Switches could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient input validation when the software processes specific SNMP object identifiers. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device. A successful exploit could allow the attacker to cause	N/A	O-CIS-IOS-060820/879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device to reload, resulting in a DoS condition. Note: To exploit this vulnerability by using SNMPv2c or earlier, the attacker must know the SNMP read-only community string for an affected system. To exploit this vulnerability by using SNMPv3, the attacker must know the user credentials for the affected system. **CVE ID : CVE-2020-3235**		
ios_xe					
Interpretation Conflict	03-06-2020	6.8	A vulnerability in the Secure Shell (SSH) server code of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload. The vulnerability is due to an internal state not being represented correctly in the SSH state machine, which leads to an unexpected behavior. An attacker could exploit this vulnerability by creating an SSH connection to an affected device and using a specific traffic pattern that causes an error condition within that connection. A successful exploit could allow an attacker to cause the device to reload, resulting in a denial of service (DoS) condition.	N/A	O-CIS-IOS_-060820/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3200		
Improper Input Validation	03-06-2020	4.9	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker with privileged EXEC credentials to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by executing crafted Tcl arguments on an affected device. An exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3201**	N/A	O-CIS-IOS_-060820/881
Uncontrolled Resource Consumption	03-06-2020	7.8	A vulnerability in the locally significant certificate (LSC) provisioning feature of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain public key infrastructure (PKI) packets. An attacker could	N/A	O-CIS-IOS_-060820/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted Secure Sockets Layer (SSL) packets to an affected device. A successful exploit could cause an affected device to continuously consume memory, which could result in a memory allocation failure that leads to a crash and causes a DoS condition. **CVE ID : CVE-2020-3203**		
Improper Input Validation	03-06-2020	7.2	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker with privileged EXEC credentials to execute arbitrary code on the underlying operating system (OS) with root privileges. The vulnerability is due to insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by loading malicious Tcl code on an affected device. A successful exploit could allow the attacker to cause memory corruption or execute the code with root privileges on the underlying OS of the affected device. **CVE ID : CVE-2020-3204**	N/A	O-CIS-IOS_-060820/883
Improper Input	03-06-2020	3.3	A vulnerability in the handling of IEEE 802.11w	N/A	O-CIS-IOS_-060820/884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Protected Management Frames (PMFs) of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to terminate a valid user connection to an affected device. The vulnerability exists because the affected software does not properly validate 802.11w disassociation and deauthentication PMFs that it receives. An attacker could exploit this vulnerability by sending a spoofed 802.11w PMF from a valid, authenticated client on a network adjacent to an affected device. A successful exploit could allow the attacker to terminate a single valid user connection to the affected device. **CVE ID : CVE-2020-3206**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing	N/A	O-CIS-IOS_-060820/885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Verification of Cryptographic Signature	03-06-2020	7.2	A vulnerability in software image verification in Cisco IOS XE Software could allow an unauthenticated, physical attacker to install and boot a malicious software image or execute unsigned binaries on an affected device. The vulnerability is due to an improper check on the area of code that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to install and boot a malicious software image or execute unsigned binaries on the targeted device. **CVE ID : CVE-2020-3209**	N/A	O-CIS-IOS_-060820/886
Improper Neutralizatio	03-06-2020	9	A vulnerability in the web UI of Cisco IOS XE Software	N/A	O-CIS-IOS_-060820/887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device. The vulnerability is due to improper input sanitization. An attacker who has valid administrative access to an affected device could exploit this vulnerability by supplying a crafted input parameter on a form in the web UI and then submitting that form. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device, which could lead to complete system compromise. **CVE ID : CVE-2020-3211**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	9	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device. The vulnerability is due to improper input sanitization. An attacker could exploit this vulnerability by uploading a crafted file to the web UI of an affected device. A successful exploit	N/A	O-CIS-IOS_-060820/888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to inject and execute arbitrary commands with root privileges on the device. **CVE ID : CVE-2020-3212**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in the ROMMON of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to those of the root user of the underlying operating system. The vulnerability is due to the ROMMON allowing for special parameters to be passed to the device at initial boot up. An attacker could exploit this vulnerability by sending parameters to the device at initial boot up. An exploit could allow the attacker to elevate from a Priv15 user to the root user and execute arbitrary commands with the privileges of the root user. **CVE ID : CVE-2020-3213**	N/A	O-CIS-IOS_-060820/889
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device.	N/A	O-CIS-IOS_-060820/890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3214		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in the Virtual Services Container of Cisco IOS XE Software could allow an authenticated, local attacker to gain root-level privileges on an affected device. The vulnerability is due to insufficient validation of a user-supplied open virtual appliance (OVA). An attacker could exploit this vulnerability by installing a malicious OVA on an affected device. **CVE ID : CVE-2020-3215**	N/A	O-CIS-IOS_-060820/891
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit	N/A	O-CIS-IOS_-060820/892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
Improper Input Validation	03-06-2020	9	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code with root privileges on the underlying Linux shell. The vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by first creating a malicious file on the affected device itself and then uploading a second malicious file to the device. A successful exploit could allow the attacker to execute arbitrary code with root privileges or bypass licensing requirements on the device. **CVE ID : CVE-2020-3218**	N/A	O-CIS-IOS_-060820/893
Improper Input Validation	03-06-2020	9	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to inject and	N/A	O-CIS-IOS_-060820/894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands with administrative privileges on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of user-supplied input to the web UI. An attacker could exploit this vulnerability by submitting crafted input to the web UI. A successful exploit could allow an attacker to execute arbitrary commands with administrative privileges on an affected device. **CVE ID : CVE-2020-3219**		
Insufficient Verification of Data Authenticity	03-06-2020	7.1	A vulnerability in the hardware crypto driver of Cisco IOS XE Software for Cisco 4300 Series Integrated Services Routers and Cisco Catalyst 9800-L Wireless Controllers could allow an unauthenticated, remote attacker to disconnect legitimate IPsec VPN sessions to an affected device. The vulnerability is due to insufficient verification of authenticity of received Encapsulating Security Payload (ESP) packets. An attacker could exploit this vulnerability by tampering with ESP cleartext values as a man-in-the-middle. **CVE ID : CVE-2020-3220**	N/A	O-CIS-IOS_-060820/895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	03-06-2020	7.8	A vulnerability in the Flexible NetFlow Version 9 packet processor of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of parameters in a Flexible NetFlow Version 9 record. An attacker could exploit this vulnerability by sending a malformed Flexible NetFlow Version 9 packet to the Control and Provisioning of Wireless Access Points (CAPWAP) data port of an affected device. An exploit could allow the attacker to trigger an infinite loop, resulting in a process crash that would cause a reload of the device. **CVE ID : CVE-2020-3221**	N/A	O-CIS-IOS_-060820/896
Improper Privilege Management	03-06-2020	3.3	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to bypass access control restrictions on an affected device. The vulnerability is due to the presence of a proxy service at a specific endpoint of the web UI. An attacker could exploit this vulnerability by	N/A	O-CIS-IOS_-060820/897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connecting to the proxy service. An exploit could allow the attacker to bypass access restrictions on the network by proxying their access request through the management network of the affected device. As the proxy is reached over the management virtual routing and forwarding (VRF), this could reduce the effectiveness of the bypass. **CVE ID : CVE-2020-3222**		
Improper Link Resolution Before File Access ('Link Following')	03-06-2020	6.8	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an authenticated, remote attacker with administrative privileges to read arbitrary files on the underlying filesystem of the device. The vulnerability is due to insufficient file scope limiting. An attacker could exploit this vulnerability by creating a specific file reference on the filesystem and then accessing it through the web UI. An exploit could allow the attacker to read arbitrary files from the underlying operating system's filesystem. **CVE ID : CVE-2020-3223**	N/A	O-CIS-IOS_-060820/898
Improper Neutralizatio n of Special	03-06-2020	9	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software	N/A	O-CIS-IOS_-060820/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			could allow an authenticated, remote attacker with read-only privileges to inject IOS commands to an affected device. The injected commands should require a higher privilege level in order to be executed. The vulnerability is due to insufficient input validation of specific HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a specific web UI endpoint on an affected device. A successful exploit could allow the attacker to inject IOS commands to the affected device, which could allow the attacker to alter the configuration of the device or cause a denial of service (DoS) condition. **CVE ID : CVE-2020-3224**		
Improper Input Validation	03-06-2020	7.8	Multiple vulnerabilities in the implementation of the Common Industrial Protocol (CIP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to insufficient input processing of CIP traffic. An attacker could exploit these	N/A	O-CIS-IOS_-060820/900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities by sending crafted CIP traffic to be processed by an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3225**		
Improper Input Validation	03-06-2020	7.8	A vulnerability in the Session Initiation Protocol (SIP) library of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient sanity checks on received SIP messages. An attacker could exploit this vulnerability by sending crafted SIP messages to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service condition. **CVE ID : CVE-2020-3226**	N/A	O-CIS-IOS_-060820/901
Incorrect Authorization	03-06-2020	10	A vulnerability in the authorization controls for the Cisco IOx application hosting infrastructure in Cisco IOS XE Software could allow an unauthenticated, remote attacker to execute Cisco IOx API commands	N/A	O-CIS-IOS_-060820/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without proper authorization. The vulnerability is due to incorrect handling of requests for authorization tokens. An attacker could exploit this vulnerability by using a crafted API call to request such a token. An exploit could allow the attacker to obtain an authorization token and execute any of the IOx API commands on an affected device. **CVE ID : CVE-2020-3227**		
Improper Input Validation	03-06-2020	7.8	A vulnerability in Security Group Tag Exchange Protocol (SXP) in Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because crafted SXP packets are mishandled. An attacker could exploit this vulnerability by sending specifically crafted SXP packets to the affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3228**	N/A	O-CIS-IOS_-060820/903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	03-06-2020	9	A vulnerability in Role Based Access Control (RBAC) functionality of Cisco IOS XE Web Management Software could allow a Read-Only authenticated, remote attacker to execute commands or configuration changes as an Admin user. The vulnerability is due to incorrect handling of RBAC for the administration GUI. An attacker could exploit this vulnerability by sending a modified HTTP request to the affected device. An exploit could allow the attacker as a Read-Only user to execute CLI commands or configuration changes as if they were an Admin user. **CVE ID : CVE-2020-3229**	N/A	O-CIS-IOS_-060820/904
Improper Input Validation	03-06-2020	5	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to prevent IKEv2 from establishing new security associations. The vulnerability is due to incorrect handling of crafted IKEv2 SA-Init packets. An attacker could exploit this vulnerability by sending crafted IKEv2 SA-Init packets to the affected device. An exploit could allow the attacker to cause	N/A	O-CIS-IOS_-060820/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device to reach the maximum incoming negotiation limits and prevent further IKEv2 security associations from being formed. **CVE ID : CVE-2020-3230**		
Improper Input Validation	03-06-2020	6.8	A vulnerability in the Simple Network Management Protocol (SNMP) implementation in Cisco ASR 920 Series Aggregation Services Router model ASR920-12SZ-IM could allow an authenticated, remote attacker to cause the device to reload. The vulnerability is due to incorrect handling of data that is returned for Cisco Discovery Protocol queries to SNMP. An attacker could exploit this vulnerability by sending a request for Cisco Discovery Protocol information by using SNMP. An exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2020-3232**	N/A	O-CIS-IOS_-060820/906
Improper Input Validation	03-06-2020	6.3	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software on Catalyst 4500 Series Switches could allow an authenticated, remote	N/A	O-CIS-IOS_-060820/907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient input validation when the software processes specific SNMP object identifiers. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: To exploit this vulnerability by using SNMPv2c or earlier, the attacker must know the SNMP read-only community string for an affected system. To exploit this vulnerability by using SNMPv3, the attacker must know the user credentials for the affected system. **CVE ID : CVE-2020-3235**		
ios_xe_sd-wan					
Improper Authentication	03-06-2020	7.2	A vulnerability in Cisco IOS XE SD-WAN Software could allow an unauthenticated, physical attacker to bypass authentication and gain unrestricted access to the root shell of an affected device. The vulnerability exists because the affected software has insufficient authentication mechanisms for certain commands. An attacker could exploit this	N/A	O-CIS-IOS_-060820/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by stopping the boot initialization of an affected device. A successful exploit could allow the attacker to bypass authentication and gain unrestricted access to the root shell of the affected device. **CVE ID : CVE-2020-3216**		
Dd-wrt					
dd-wrt					
Cross-Site Request Forgery (CSRF)	09-06-2020	6.8	** DISPUTED ** An issue was discovered in DD-WRT through 16214. The Diagnostic page allows remote attackers to execute arbitrary commands via shell metacharacters in the host field of the ping command. Exploitation through CSRF might be possible. NOTE: software maintainers consider the report invalid because it refers to an old software version, requires administrative privileges, and does not provide access beyond that already available to administrative users. **CVE ID : CVE-2020-13976**	N/A	O-DD--DD-W-060820/909
Debian					
debian_linux					
Out-of-bounds Read	11-06-2020	6.4	In exif_entry_get_value of exif-entry.c, there is a possible out of bounds read due to a missing bounds	N/A	O-DEB-DEBI-060820/910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-147140917 **CVE ID : CVE-2020-0182**		
Integer Overflow or Wraparound	11-06-2020	5	In exif_data_load_data_content of exif-data.c, there is a possible UBSAN abort due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-146428941 **CVE ID : CVE-2020-0198**	N/A	O-DEB-DEBI-060820/911
Use of a Broken or Risky Cryptographic Algorithm	04-06-2020	5.8	GnuTLS 3.6.x before 3.6.14 uses incorrect cryptography for encrypting a session ticket (a loss of confidentiality in TLS 1.2, and an authentication bypass in TLS 1.3). The earliest affected version is 3.6.4 (2018-09-24) because of an error in a 2018-09-18 commit. Until the first key rotation, the TLS server always uses wrong data in place of an encryption key derived from an application. **CVE ID : CVE-2020-13777**	https://gnutls.org/security-new.html#GNUTLS-SA-2020-06-03, https://security.netapp.com/advisory/ntap-20200619-0004/	O-DEB-DEBI-060820/912
Information	06-06-2020	4.3	In support.c in pam_tacplus	N/A	O-DEB-DEBI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure Through Log Files			1.3.8 through 1.5.1, the TACACS+ shared secret gets logged via syslog if the DEBUG loglevel and journald are used. **CVE ID : CVE-2020-13881**		060820/913
Improper Privilege Management	09-06-2020	6.9	A flaw was found in the Linux Kernel in versions after 4.5-rc1 in the way mremap handled DAX Huge Pages. This flaw allows a local attacker with access to a DAX enabled storage to escalate their privileges on the system. **CVE ID : CVE-2020-10757**	https://security.netapp.com/advisory/ntap-20200702-0004/	O-DEB-DEBI-060820/914
Improper Enforcement of Message or Data Structure	03-06-2020	5	In nghttp2 before version 1.41.0, the overly large HTTP/2 SETTINGS frame payload causes denial of service. The proof of concept attack involves a malicious client constructing a SETTINGS frame with a length of 14,400 bytes (2400 individual settings entries) over and over again. The attack causes the CPU to spike at 100%. nghttp2 v1.41.0 fixes this vulnerability. There is a workaround to this vulnerability. Implement nghttp2_on_frame_recv_callback callback, and if received frame is SETTINGS frame and the number of settings entries are large (e.g., > 32), then drop the connection.	https://github.com/nghttp2/nghttp2/security/advisories/GHSA-q5wr-xfw9-q7xr	O-DEB-DEBI-060820/915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11080		
Incorrect Permission Assignment for Critical Resource	08-06-2020	3.6	An issue was discovered in LinuxTV xawtv before 3.107. The function dev_open() in v4l-conf.c does not perform sufficient checks to prevent an unprivileged caller of the program from opening unintended filesystem paths. This allows a local attacker with access to the v4l-conf setuid-root program to test for the existence of arbitrary files and to trigger an open on arbitrary files with mode O_RDWR. To achieve this, relative path components need to be added to the device path, as demonstrated by a v4l-conf -c /dev/../root/.bash_history command. **CVE ID : CVE-2020-13696**	http://www.openwall.com/lists/oss-security/2020/06/04/6	O-DEB-DEBI-060820/916
NULL Pointer Dereference	04-06-2020	5	Portable UPnP SDK (aka libupnp) 1.12.1 and earlier allows remote attackers to cause a denial of service (crash) via a crafted SSDP message due to a NULL pointer dereference in the functions FindServiceControlURLPath and FindServiceEventURLPath in genlib/service_table/service_table.c. **CVE ID : CVE-2020-13848**	N/A	O-DEB-DEBI-060820/917
Dell					
g3_15_3590_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-G3_1-060820/918
g5_15_5590_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-G5_1-060820/919
g5_5090_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	O-DEL-G5_5-060820/920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
g7_15_7590_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-G7_1-060820/921
g7_17_7790_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-G7_1-060820/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
inspiron_14_5490_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/923
inspiron_3490_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/924
inspiron_3493_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	O-DEL-INSP-060820/925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_3590_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/926
inspiron_3593_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	O-DEL-INSP-060820/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_3790_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/928
inspiron_3793_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/929
inspiron_5390_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	O-DEL-INSP-060820/930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5391_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/931
inspiron_5493_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	O-DEL-INSP-060820/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5494_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/933
inspiron_5498_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
inspiron_5583_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/935
inspiron_5584_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/936
inspiron_5590_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	O-DEL-INSP-060820/937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5593_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/938
inspiron_5594_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	O-DEL-INSP-060820/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
inspiron_5598_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/940
inspiron_7391_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/941
inspiron_7490_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	O-DEL-INSP-060820/942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_7590_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/943
inspiron_7591_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	O-DEL-INSP-060820/944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3301_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/945
latitude_3300_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/946
latitude_3400_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/947
latitude_3500_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/948
latitude_5300_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the	N/A	O-DEL-LATI-060820/949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**		
latitude_5400_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-LATI-060820/950
latitude_5401_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an	N/A	O-DEL-LATI-060820/951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**		
latitude_5420_rugged_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/952
latitude_5424_rugged_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
latitude_5500_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-LATI-060820/954
latitude_5501_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-LATI-060820/955
latitude_7220ex_rugged_extreme_tablet_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms	N/A	O-DEL-LATI-060820/956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**		
latitude_7300_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-LATI-060820/957
latitude_7400_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's	N/A	O-DEL-LATI-060820/958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**		
precision_3540_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-PREC-060820/959
precision_3541_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS	N/A	O-DEL-PREC-060820/960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-PREC-060820/961
precision_5540_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-PREC-060820/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
precision_7540_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-PREC-060820/963
precision_7730_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/964
precision_7740_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows	N/A	O-DEL-PREC-060820/965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**		
vostro_15_7580_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/966
vostro_3481_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS	N/A	O-DEL-VOST-060820/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3490_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/968
vostro_3590_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vostro_5390_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/970
vostro_5391_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/971
vostro_5490_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	O-DEL-VOST-060820/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_5590_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/973
vostro_7590_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	O-DEL-VOST-060820/974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
wyse_5070_thin_client_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-WYSE-060820/975
wyse_5470_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-WYSE-060820/976
xps_13_9380_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	O-DEL-XPS_-060820/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
xps_15_9570_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-XPS_-060820/978
inspiron_14_gaming_7466_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	O-DEL-INSP-060820/979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_14_gaming_7467_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/980
inspiron_15_7572_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/981
inspiron_15_gaming_7566_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/982
inspiron_15_gaming_7567_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/983
inspiron_15_gaming_7577_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	O-DEL-INSP-060820/984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
chengming_3967_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-CHEN-060820/985
g7_7588_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-G7_7-060820/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
latitude_3460_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/987
latitude_3470_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/988
latitude_3480_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	O-DEL-LATI-060820/989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3490_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/990
latitude_3560_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	O-DEL-LATI-060820/991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3570_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/992
latitude_3580_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/993
latitude_3590_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	O-DEL-LATI-060820/994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5175_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/995
latitude_5179_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	O-DEL-LATI-060820/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5250_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/997
latitude_5280_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
latitude_5285_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/999
latitude_5288_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1000
latitude_5289_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	O-DEL-LATI-060820/1001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5290_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1002
latitude_5290_2-in-1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	O-DEL-LATI-060820/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
latitude_5450_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1004
latitude_5480_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1005
latitude_5488_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	O-DEL-LATI-060820/1006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5490_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1007
latitude_5491_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	O-DEL-LATI-060820/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5550_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1009
precision_5510_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1010
precision_5520_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1011
precision_5530_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1012
precision_5720_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	O-DEL-PREC-060820/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_7510_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1014
precision_7520_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-PREC-060820/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
precision_7530_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1016
precision_7710_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1017
precision_7720_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	O-DEL-PREC-060820/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_7820_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1019
precision_7920_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	O-DEL-PREC-060820/1020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3070_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1021
vostro_3267_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1022
vostro_3268_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	O-DEL-VOST-060820/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
chengming_3977_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-CHEN-060820/1024
chengming_3980_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	O-DEL-CHEN-060820/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
g3_3579_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-G3_3-060820/1026
g5_5587_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-G5_5-060820/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xps_8900_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-XPS_-060820/1028
g3_3779_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-G3_3-060820/1029
embedded_box_pc_5000_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	O-DEL-EMBE-060820/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5580_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1031
latitude_5590_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	O-DEL-LATI-060820/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
latitude_5591_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1033
latitude_7250_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1034
latitude_7275_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	O-DEL-LATI-060820/1035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_7280_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1036
latitude_7285_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	O-DEL-LATI-060820/1037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_7290_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1038
latitude_7350_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1039
latitude_7370_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1040
latitude_7380_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1041
latitude_7389_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	O-DEL-LATI-060820/1042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_7390_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1043
latitude_7390_2-in-1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-LATI-060820/1044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
latitude_7424_rugged_extreme_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1045
latitude_7480_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1046
latitude_7490_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	O-DEL-LATI-060820/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_e5250_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1048
latitude_e5270_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	O-DEL-LATI-060820/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_e5450_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1050
latitude_e5470_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1051
latitude_e5550_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	O-DEL-LATI-060820/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_e5570_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1053
latitude_e7250_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	O-DEL-LATI-060820/1054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_e7270_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1055
latitude_e7450_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
latitude_e7470_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1057
optiplex_3040_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1058
optiplex_3046_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	O-DEL-OPTI-060820/1059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_3050_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1060
optiplex_3050_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	O-DEL-OPTI-060820/1061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
optiplex_3060_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1062
optiplex_3240_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1063
optiplex_5040_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	O-DEL-OPTI-060820/1064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_5050_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1065
optiplex_5060_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	O-DEL-OPTI-060820/1066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_5260_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1067
optiplex_7040_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1068
optiplex_7050_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1069
optiplex_7060_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1070
optiplex_7440_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	O-DEL-OPTI-060820/1071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_7460_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1072
optiplex_7760_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-OPTI-060820/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
optiplex_xe3_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1074
precision_3430_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1075
precision_3510_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	O-DEL-PREC-060820/1076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_3520_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1077
precision_3530_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	O-DEL-PREC-060820/1078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_5530_2-in_1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1079
precision_5550_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1080
precision_5820_tower_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	O-DEL-PREC-060820/1081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_7820_tower_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1082
precision_7920_tower_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	O-DEL-PREC-060820/1083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_tower_3431_small_form_factor_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1084
vostro_14_3468_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vostro_14_3478_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1086
vostro_14_5468_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1087
vostro_15_3568_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	O-DEL-VOST-060820/1088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_15_3578_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1089
vostro_15_5568_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	O-DEL-VOST-060820/1090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
vostro_3471_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1091
vostro_3491_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1092
vostro_3558_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	O-DEL-VOST-060820/1093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3559_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1094
vostro_3591_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	O-DEL-VOST-060820/1095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3671_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1096
vostro_3681_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1097
vostro_3881_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1098
vostro_3888_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1099
vostro_5090_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	O-DEL-VOST-060820/1100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_5300_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1101
vostro_5880_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-VOST-060820/1102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
vostro_7500_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1103
wyse_5470_all-in-one_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-WYSE-060820/1104
wyse_7040_thin_client_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	O-DEL-WYSE-060820/1105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
xps_13_9370_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-XPS_-060820/1106
inspiron_3670_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	O-DEL-INSP-060820/1107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_3070_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1108
optiplex_5070_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1109
optiplex_5250_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	O-DEL-OPTI-060820/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_7070_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1111
optiplex_7450_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	O-DEL-OPTI-060820/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_15_7570_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1113
xps_12_9250_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-XPS_-060820/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xps_13_9360_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-XPS_-060820/1115
xps_15_9560_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-XPS_-060820/1116
chengming_3988_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	O-DEL-CHEN-060820/1117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
chengming_3990_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-CHEN-060820/1118
chengming_3991_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	O-DEL-CHEN-060820/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
g3_15_3500_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-G3_1-060820/1120
g5_15_5500_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-G5_1-060820/1121
inspiron_11_2-in-1_3153_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	O-DEL-INSP-060820/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_11_2-in-1_3158_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1123
inspiron_13_7370_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	O-DEL-INSP-060820/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_13_2-in-1_5368_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1125
inspiron_13_2-in-1_5378_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1126
inspiron_13_2-in-1_5379_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1127
inspiron_13_2-in-1_7353_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1128
inspiron_13_2-in-1_7359_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	O-DEL-INSP-060820/1129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_13_2-in-1_7368_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1130
inspiron_13_2-in-1_7373_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-INSP-060820/1131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
inspiron_13_2-in-1_7378_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1132
inspiron_14_3458_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1133
inspiron_14_3459_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	O-DEL-INSP-060820/1134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_14_3467_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1135
inspiron_14_3468_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	O-DEL-INSP-060820/1136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_14_3473_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1137
inspiron_14_5468_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1138
inspiron_14_7460_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	O-DEL-INSP-060820/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_15_3559_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1140
xps_13_2-in-1_9365_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	O-DEL-XPS_-060820/1141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
xps_13_9300_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-XPS_-060820/1142
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-XPS_-060820/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xps_15_2-in-1_9575_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-XPS_-060820/1144
xps_15_7500_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-XPS_-060820/1145
xps_27_aio_7760_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	O-DEL-XPS_-060820/1146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
xps_7380_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-XPS_-060820/1147
xps_7390_2-in-1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	O-DEL-XPS_-060820/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-XPS_-060820/1149
latitude_7200_2_in_1_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-LATI-060820/1150
latitude_7220_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-LATI-060820/1151
xps_7590_firmware					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-XPS_-060820/1152
inspiron_3268_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	O-DEL-INSP-060820/1153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_3470_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1154
inspiron_3476_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	O-DEL-INSP-060820/1155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_3480_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1156
inspiron_3481_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1157
inspiron_3576_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1158
inspiron_3580_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1159
inspiron_3583_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	O-DEL-INSP-060820/1160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_3581_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1161
inspiron_3584_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-INSP-060820/1162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
inspiron_3668_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1163
inspiron_3780_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1164
inspiron_3781_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	O-DEL-INSP-060820/1165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5370_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1166
inspiron_5457_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	O-DEL-INSP-060820/1167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_15_3567_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1168
inspiron_15_3568_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1169
inspiron_15_5566_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	O-DEL-INSP-060820/1170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_15_5567_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1171
inspiron_15_7560_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	O-DEL-INSP-060820/1172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_15_7570_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1173
inspiron_15_2-in-1_5568_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
inspiron_15_2-in-1_5578_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1175
inspiron_15_2-in-1_5579_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1176
inspiron_15_2-in-1_7568_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	O-DEL-INSP-060820/1177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_15_2-in-1_7569_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1178
inspiron_15_2-in-1_7573_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	O-DEL-INSP-060820/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
inspiron_15_2-in-1_7579_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1180
inspiron_15-3552_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1181
inspiron_17_5767_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	O-DEL-INSP-060820/1182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_17_2-in-1_7773_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1183
inspiron_17_2-in-1_7778_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	O-DEL-INSP-060820/1184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_17_2-in-1_7779_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1185
inspiron_3471_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1186
inspiron_3671_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1187
inspiron_3880_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1188
inspiron_3881_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	O-DEL-INSP-060820/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5300_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1190
inspiron_5400_2_in1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-INSP-060820/1191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
inspiron_5491_2_in_1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1192
inspiron_5591_2-in-1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1193
inspiron_5459_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	O-DEL-INSP-060820/1194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5480_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1195
inspiron_5481_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	O-DEL-INSP-060820/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5482_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1197
inspiron_5557_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1198
inspiron_5559_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	O-DEL-INSP-060820/1199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5570_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1200
inspiron_5580_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	O-DEL-INSP-060820/1201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5582_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1202
inspiron_5759_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
inspiron_5770_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1204
inspiron_7380_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1205
inspiron_7386_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	O-DEL-INSP-060820/1206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_7472_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1207
inspiron_7580_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	O-DEL-INSP-060820/1208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
inspiron_7586_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1209
inspiron_7786_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1210
latitude_3180_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	O-DEL-LATI-060820/1211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3189_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1212
latitude_3190_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	O-DEL-LATI-060820/1213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3350_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1214
latitude_3379_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1215
latitude_3380_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1216
inspiron_7300_2_in_1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1217
inspiron_7390_2_in_1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	O-DEL-INSP-060820/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_7391_2_in_1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1219
inspiron_7500_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-INSP-060820/1220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
inspiron_7500_2_in_1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1221
inspiron_7501_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1222
inspiron_7590_2_in_1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	O-DEL-INSP-060820/1223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_7591_2_in_1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1224
inspiron_5490_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	O-DEL-INSP-060820/1225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_7790_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1226
insprion_5491_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-INSP-060820/1227
latitude_3190_2-in-1_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	O-DEL-LATI-060820/1228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3310_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1229
latitude_3310_2-in-1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	O-DEL-LATI-060820/1230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3390_2-in-1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1231
latitude_3410_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
latitude_3460_mobile_thin_client_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1233
latitude_3480_mobile_thin_client_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1234
latitude_3510_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	O-DEL-LATI-060820/1235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5280_mobile_thin_client_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1236
latitude_5300_2-in-1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	O-DEL-LATI-060820/1237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	O-DEL-LATI-060820/1238
latitude_5310_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1239
latitude_5310_2_in_1_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	O-DEL-LATI-060820/1240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5410_firmware					
Missing Authorizatio n	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1241
latitude_5411_firmware					
Missing Authorizatio n	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	O-DEL-LATI-060820/1242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5414_rugged_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1243
latitude_5510_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1244
latitude_5511_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1245
latitude_7210_2_in_1_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1246
latitude_7212_rugged_extreme_tablet_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	O-DEL-LATI-060820/1247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_7214_rugged_extreme_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1248
latitude_7310_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-LATI-060820/1249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
latitude_7410_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1250
latitude_7414_rugged_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1251
latitude_9410_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	O-DEL-LATI-060820/1252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_9510_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-LATI-060820/1253
latitude_e7270_mobile_thin_client_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	O-DEL-LATI-060820/1254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_3280_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1255
optiplex_5080_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1256
optiplex_5270_aio_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	O-DEL-OPTI-060820/1257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_5480_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1258
optiplex_7071_tower_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	O-DEL-OPTI-060820/1259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_7080_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1260
optiplex_7480_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
optiplex_7780_aio_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1262
optiplex_aio_7470_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-OPTI-060820/1263
optiplex_aio_7770_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	O-DEL-OPTI-060820/1264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_3420_tower_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1265
precision_3440_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	O-DEL-PREC-060820/1266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
precision_3550_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1267
precision_3551_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1268
precision_3620_tower_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	O-DEL-PREC-060820/1269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_3630_tower_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1270
precision_3640_tower_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	O-DEL-PREC-060820/1271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_3930_rack_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-PREC-060820/1272
vostro_3458_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1273
vostro_3459_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1274
vostro_3470_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1275
vostro_3480_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	O-DEL-VOST-060820/1276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3580_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1277
vostro_3581_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	O-DEL-VOST-060820/1278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
vostro_3584_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1279
vostro_3583_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1280
vostro_3660_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	O-DEL-VOST-060820/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3667_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1282
vostro_3668_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	O-DEL-VOST-060820/1283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3669_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1284
vostro_3670_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1285
vostro_5370_firmware					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	O-DEL-VOST-060820/1286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_5471_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1287
vostro_5481_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	O-DEL-VOST-060820/1288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_5581_firmware					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	O-DEL-VOST-060820/1289
Digi					
saros					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors.	N/A	O-DIG-SARO-060820/1290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10136		
Dlink					
dsl-2730u_firmware					
N/A	08-06-2020	5	D-Link DSL 2730-U IN_1.10 and IN_1.11 and DIR-600M 3.04 devices have the domain.name string in the DNS resolver search path by default, which allows remote attackers to provide valid DNS responses (and also offer Internet services such as HTTP) for names that otherwise would have had an NXDOMAIN error, by registering a subdomain of the domain.name domain name. **CVE ID : CVE-2020-13960**	N/A	O-DLI-DSL--060820/1291
dir-865l_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.5	D-Link DIR-865L Ax 1.20B01 Beta devices allow Command Injection. **CVE ID : CVE-2020-13782**	N/A	O-DLI-DIR--060820/1292
Information Exposure	03-06-2020	5	D-Link DIR-865L Ax 1.20B01 Beta devices have Cleartext Storage of Sensitive Information. **CVE ID : CVE-2020-13783**	N/A	O-DLI-DIR--060820/1293
Use of Cryptographically Weak Pseudo-	03-06-2020	5	D-Link DIR-865L Ax 1.20B01 Beta devices have a predictable seed in a Pseudo-Random Number	N/A	O-DLI-DIR--060820/1294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Random Number Generator (PRNG)			Generator. **CVE ID : CVE-2020-13784**		
Inadequate Encryption Strength	03-06-2020	5	D-Link DIR-865L Ax 1.20B01 Beta devices have Inadequate Encryption Strength. **CVE ID : CVE-2020-13785**	N/A	O-DLI-DIR--060820/1295
Cross-Site Request Forgery (CSRF)	03-06-2020	6.8	D-Link DIR-865L Ax 1.20B01 Beta devices allow CSRF. **CVE ID : CVE-2020-13786**	N/A	O-DLI-DIR--060820/1296
Information Exposure	03-06-2020	5	D-Link DIR-865L Ax 1.20B01 Beta devices have Cleartext Transmission of Sensitive Information. **CVE ID : CVE-2020-13787**	N/A	O-DLI-DIR--060820/1297
dir-600m_firmware					
N/A	08-06-2020	5	D-Link DSL 2730-U IN_1.10 and IN_1.11 and DIR-600M 3.04 devices have the domain.name string in the DNS resolver search path by default, which allows remote attackers to provide valid DNS responses (and also offer Internet services such as HTTP) for names that otherwise would have had an NXDOMAIN error, by registering a subdomain of the domain.name domain name. **CVE ID : CVE-2020-13960**	N/A	O-DLI-DIR--060820/1298
dsl-2750u_firmware					
Missing Authenticati	15-06-2020	4.6	D-link DSL-2750U ISL2750UEME3.V1E devices	N/A	O-DLI-DSL--060820/1299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on for Critical Function			allow approximately 90 seconds of access to the control panel, after a restart, before MAC address filtering rules become active. **CVE ID : CVE-2020-13150**		
Fedoraproject					
fedora					
Integer Overflow or Wraparound	05-06-2020	7.5	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection. **CVE ID : CVE-2020-10878**	https://github.com/Perl/perl5/blob/blead/pod/perl5303delta.pod, https://github.com/perl/perl5/commit/0a320d753fe7fca03df259a4dfd8e641e51edaa8, https://github.com/perl/perl5/commit/3295b48defa0f8570114877b063fe546dd348b3c	O-FED-FEDO-060820/1300
Use of a Broken or Risky Cryptographic Algorithm	04-06-2020	5.8	GnuTLS 3.6.x before 3.6.14 uses incorrect cryptography for encrypting a session ticket (a loss of confidentiality in TLS 1.2, and an authentication bypass in TLS 1.3). The earliest affected version is 3.6.4 (2018-09-24) because of an error in a 2018-09-18	https://gnutls.org/security-new.html#GNUTLS-SA-2020-06-03, https://security.netapp.com/advi	O-FED-FEDO-060820/1301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commit. Until the first key rotation, the TLS server always uses wrong data in place of an encryption key derived from an application. **CVE ID : CVE-2020-13777**	sory/ntap-20200619-0004/	
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	O-FED-FEDO-060820/1302
Out-of-bounds Write	05-06-2020	6.4	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow. **CVE ID : CVE-2020-10543**	https://github.com/Perl/perl5/blob/blead/pod/perl5303delta.pod, https://github.com/perl/perl5/commit/897d1f7fd515b828e4b198d8b8bef76c6faf03ed, https://github.com/Perl/perl5/compare/v5.30.2...v5.30.3	O-FED-FEDO-060820/1303
Improper Authentication	08-06-2020	4	It was found that nmcli, a command line interface to NetworkManager did not honour 802-1x.ca-path and 802-1x.phase2-ca-path settings, when creating a	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-	O-FED-FEDO-060820/1304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			new profile. When a user connects to a network using this profile, the authentication does not happen and the connection is made insecurely. **CVE ID : CVE-2020-10754**	10754	
Improper Privilege Management	09-06-2020	6.9	A flaw was found in the Linux Kernel in versions after 4.5-rc1 in the way mremap handled DAX Huge Pages. This flaw allows a local attacker with access to a DAX enabled storage to escalate their privileges on the system. **CVE ID : CVE-2020-10757**	https://security.netapp.com/advisory/ntap-20200702-0004/	O-FED-FEDO-060820/1305
Server-Side Request Forgery (SSRF)	03-06-2020	6.4	The avatar feature in Grafana 3.0.1 through 7.0.1 has an SSRF Incorrect Access Control issue. This vulnerability allows any unauthenticated user/client to make Grafana send HTTP requests to any URL and return its result to the user/client. This can be used to gain information about the network that Grafana is running on. Furthermore, passing invalid URL objects could be used for DOS'ing Grafana via SegFault. **CVE ID : CVE-2020-13379**	http://www.openwall.com/lists/oss-security/2020/06/03/4, https://grafana.com/blog/2020/06/03/grafana-6.7.4-and-7.0.2-released-with-important-security-fix/, https://security.netapp.com/advisory/ntap-20200608-	O-FED-FEDO-060820/1306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				0006/	
Authentication Bypass Using an Alternate Path or Channel	12-06-2020	6	In affected versions of WordPress, misuse of the `set-screen-option` filter's return value allows arbitrary user meta fields to be saved. It does require an admin to install a plugin that would misuse the filter. Once installed, it can be leveraged by low privileged users. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34). **CVE ID : CVE-2020-4050**	https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4vpv-fgg2-gcqc	O-FED-FEDO-060820/1307
Freebsd					
freebsd					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.2	In FreeBSD 12.1-STABLE before r361918, 12.1-RELEASE before p6, 11.4-STABLE before r361919, 11.3-RELEASE before p10, and 11.4-RC2 before p1, an invalid memory location may be used for HID items if the push/pop level is not restored within the processing of that HID item allowing an attacker with physical access to a USB port to be able to use a specially crafted USB device to gain kernel or user-space code execution.	https://security.netapp.com/advisory/ntap-20200625-0005/	O-FRE-FREE-060820/1308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7456		
Use of Externally-Controlled Format String	09-06-2020	7.5	AnyDesk before 5.5.3 on Linux and FreeBSD has a format string vulnerability that can be exploited for remote code execution. **CVE ID : CVE-2020-13160**	N/A	O-FRE-FREE-060820/1309
GE					
rt430_firmware					
Missing Authentication for Critical Function	02-06-2020	9	GE Grid Solutions Reason RT Clocks, RT430, RT431, and RT434, all firmware versions prior to 08A05. The device's vulnerability in the web application could allow multiple unauthenticated attacks that could cause serious impact. The vulnerability may allow an unauthenticated attacker to execute arbitrary commands and send a request to a specific URL that could cause the device to become unresponsive. The unauthenticated attacker may change the password of the 'configuration' user account, allowing the attacker to modify the configuration of the device via the web interface using the new password. This vulnerability may also allow an unauthenticated attacker to bypass the authentication required to configure the device and reboot the system.	N/A	O-GE-RT43-060820/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12017		
rt431_firmware					
Missing Authentication for Critical Function	02-06-2020	9	GE Grid Solutions Reason RT Clocks, RT430, RT431, and RT434, all firmware versions prior to 08A05. The device's vulnerability in the web application could allow multiple unauthenticated attacks that could cause serious impact. The vulnerability may allow an unauthenticated attacker to execute arbitrary commands and send a request to a specific URL that could cause the device to become unresponsive. The unauthenticated attacker may change the password of the 'configuration' user account, allowing the attacker to modify the configuration of the device via the web interface using the new password. This vulnerability may also allow an unauthenticated attacker to bypass the authentication required to configure the device and reboot the system. **CVE ID : CVE-2020-12017**	N/A	O-GE-RT43-060820/1311
rt434_firmware					
Missing Authentication for Critical Function	02-06-2020	9	GE Grid Solutions Reason RT Clocks, RT430, RT431, and RT434, all firmware versions prior to 08A05. The device's vulnerability in the web application could allow	N/A	O-GE-RT43-060820/1312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple unauthenticated attacks that could cause serious impact. The vulnerability may allow an unauthenticated attacker to execute arbitrary commands and send a request to a specific URL that could cause the device to become unresponsive. The unauthenticated attacker may change the password of the 'configuration' user account, allowing the attacker to modify the configuration of the device via the web interface using the new password. This vulnerability may also allow an unauthenticated attacker to bypass the authentication required to configure the device and reboot the system. **CVE ID : CVE-2020-12017**		
Google					
chrome_os					
Use After Free	12-06-2020	10	Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/flash-player/apsb20-30.html	O-GOO-CHRO-060820/1313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9633		
android					
Out-of-bounds Read	11-06-2020	4.3	In GetOpusHeaderBuffers() of OpusHeader.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142861738 **CVE ID : CVE-2020-0180**	N/A	O-GOO-ANDR-060820/1314
Integer Overflow or Wraparound	11-06-2020	5	In exif_data_load_data_thumbnail of exif-data.c, there is a possible denial of service due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145075076 **CVE ID : CVE-2020-0181**	N/A	O-GOO-ANDR-060820/1315
Out-of-bounds Read	11-06-2020	6.4	In exif_entry_get_value of exif-entry.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	N/A	O-GOO-ANDR-060820/1316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-10Android ID: A-147140917 **CVE ID : CVE-2020-0182**		
Improper Privilege Management	11-06-2020	4.4	In handleMessage of BluetoothManagerService, there is an incomplete reset. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-110181479 **CVE ID : CVE-2020-0183**	N/A	O-GOO-ANDR-060820/1317
Loop with Unreachable Exit Condition ('Infinite Loop')	11-06-2020	4.3	In ihevcd_ref_list() of ihevcd_ref_list.c, there is a possible infinite loop due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141688974 **CVE ID : CVE-2020-0184**	N/A	O-GOO-ANDR-060820/1318
Out-of-bounds Read	11-06-2020	2.1	In avrc_pars_browsing_cmd of avrc_pars_tg.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-79945152	N/A	O-GOO-ANDR-060820/1319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0185		
Out-of-bounds Write	11-06-2020	4.6	In hal_fd_init of hal_fd.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-146144463 **CVE ID : CVE-2020-0186**	N/A	O-GOO-ANDR-060820/1320
N/A	11-06-2020	2.1	In engineSetMode of BaseBlockCipher.java, there is a possible incorrect cryptographic algorithm chosen due to an incomplete comparison. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-148517383 **CVE ID : CVE-2020-0187**	N/A	O-GOO-ANDR-060820/1321
Improper Privilege Management	11-06-2020	4.6	In onCreatePermissionRequest of SettingsSliceProvider.java, there is a possible permissions bypass due to a PendingIntent error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for	N/A	O-GOO-ANDR-060820/1322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10Android ID: A-147355897 **CVE ID : CVE-2020-0188**		
Loop with Unreachable Exit Condition ('Infinite Loop')	11-06-2020	4.3	In ihevcd_decode() of ihevcd_decode.c, there is possible resource exhaustion due to an infinite loop. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139939283 **CVE ID : CVE-2020-0189**	N/A	O-GOO-ANDR-060820/1323
Out-of-bounds Read	11-06-2020	6.8	In ideint_weave_blk of ideint_utils.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140324890 **CVE ID : CVE-2020-0190**	N/A	O-GOO-ANDR-060820/1324
Out-of-bounds Read	11-06-2020	4.3	In ih264d_update_default_index_list() of ih264d_dpb_mgr.c, there is a possible out of bounds read due to a logic error. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed	N/A	O-GOO-ANDR-060820/1325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for exploitation.Product: AndroidVersions: Android-10Android ID: A-140561484 **CVE ID : CVE-2020-0191**		
Out-of-bounds Read	11-06-2020	4.3	In ih264d_decode_slice_thread of ih264d_thread_parse_decode.c, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-144687080 **CVE ID : CVE-2020-0192**	N/A	O-GOO-ANDR-060820/1326
Out-of-bounds Read	11-06-2020	4.3	In ihevc_intra_pred_chroma_mode_3_to_9_av8 of ihevc_intra_pred_chroma_mode_3_to_9.s, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-144595488 **CVE ID : CVE-2020-0193**	N/A	O-GOO-ANDR-060820/1327
Integer Overflow or Wraparound	11-06-2020	6.8	In ihevcd_parse_slice_header of ihevcd_parse_slice_header.c,	N/A	O-GOO-ANDR-060820/1328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143826590 **CVE ID : CVE-2020-0194**		
Information Exposure	11-06-2020	4.3	In ihevcd_iquant_itrans_recon_ctb of ihevcd_iquant_itrans_recon_ctb.c and related functions, there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-144686961 **CVE ID : CVE-2020-0195**	N/A	O-GOO-ANDR-060820/1329
Improper Input Validation	11-06-2020	3.3	In RegisterNotificationResponse::GetEvent of register_notification_packet.cc, there is a possible abort due to improper input validation. This could lead to remote denial of service of the Bluetooth service, over Bluetooth, with no additional execution privileges needed. User	N/A	O-GOO-ANDR-060820/1330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-144066833 **CVE ID : CVE-2020-0196**		
Out-of-bounds Read	11-06-2020	2.1	In InitDataParser::parsePssh of InitDataParser.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-137370379 **CVE ID : CVE-2020-0197**	N/A	O-GOO-ANDR-060820/1331
Integer Overflow or Wraparound	11-06-2020	5	In exif_data_load_data_content of exif-data.c, there is a possible UBSAN abort due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-146428941 **CVE ID : CVE-2020-0198**	N/A	O-GOO-ANDR-060820/1332
Use After Free	11-06-2020	1.9	In TimeCheck::TimeCheckThread::threadLoop of TimeCheck.cpp, there is a possible use-after-free due to a race condition. This could lead to local	N/A	O-GOO-ANDR-060820/1333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142142406 **CVE ID : CVE-2020-0199**		
Out-of-bounds Read	11-06-2020	4.3	In ReadLittleEndian of raw_bit_reader.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure in the media server with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-147231862 **CVE ID : CVE-2020-0200**	N/A	O-GOO-ANDR-060820/1334
Improper Privilege Management	11-06-2020	7.5	In showSecurityFields of WifiConfigController.java there is a possible credential leak due to a confused deputy. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143601727 **CVE ID : CVE-2020-0201**	N/A	O-GOO-ANDR-060820/1335
Incorrect Default Permissions	11-06-2020	6.8	In onStart of MainActivity.java, there is a possible bypass of developer	N/A	O-GOO-ANDR-060820/1336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings requirements for capturing system traces due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142936525 **CVE ID : CVE-2020-0202**		
Improper Privilege Management	11-06-2020	4.6	In freeIsolatedUidLocked of ProcessList.java, there is a possible UID reuse due to improper cleanup. This could lead to local escalation of privilege between constrained processes with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-146313311 **CVE ID : CVE-2020-0203**	N/A	O-GOO-ANDR-060820/1337
Deserialization of Untrusted Data	11-06-2020	2.1	In BnAAudioService::onTransact of IAAudioService.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139473816	N/A	O-GOO-ANDR-060820/1338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0132		
Incorrect Default Permissions	11-06-2020	4.4	In MockLocationAppPreference Controller.java, it is possible to mock the GPS location of the device due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145136060 **CVE ID : CVE-2020-0133**	N/A	O-GOO-ANDR-060820/1339
Information Exposure	11-06-2020	2.1	In BnDrm::onTransact of IDrm.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-146052771 **CVE ID : CVE-2020-0134**	N/A	O-GOO-ANDR-060820/1340
Incorrect Default Permissions	11-06-2020	2.1	In dump of RollbackManagerServiceImpl.java, there is a possible backup metadata exposure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-	N/A	O-GOO-ANDR-060820/1341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10Android ID: A-150949837 **CVE ID : CVE-2020-0135**		
Integer Overflow or Wraparound	11-06-2020	4.6	In multiple locations of Parcel.cpp, there is a possible out-of-bounds write due to an integer overflow. This could lead to local escalation of privilege in the system server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-120078455 **CVE ID : CVE-2020-0136**	N/A	O-GOO-ANDR-060820/1342
Incorrect Default Permissions	11-06-2020	4.6	In setIPv6AddrGenMode of NetworkManagementService .java, there is a possible bypass of networking permissions due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141920289 **CVE ID : CVE-2020-0137**	N/A	O-GOO-ANDR-060820/1343
Out-of-bounds Write	11-06-2020	6.8	In get_element_attr_rsp of btif_rc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution if bluetoothtbd were used, which it isn't in typical Android platforms,	N/A	O-GOO-ANDR-060820/1344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142878416 **CVE ID : CVE-2020-0138**		
Integer Overflow or Wraparound	11-06-2020	2.1	In NDEF_MsgValidate of ndef_utils.c, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure if a malformed NFC tag is provided by the firmware. System execution privileges are needed and user interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145520471 **CVE ID : CVE-2020-0139**	N/A	O-GOO-ANDR-060820/1345
Information Exposure	11-06-2020	5	In rw_i93_sm_detect_ndef of rw_i93.c, there is a possible information disclosure due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-146053215 **CVE ID : CVE-2020-0140**	N/A	O-GOO-ANDR-060820/1346
Information Exposure	11-06-2020	2.1	In OutputBuffersArray::realloc of CCodecBuffers.cpp, there is a possible heap disclosure	N/A	O-GOO-ANDR-060820/1347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to a race condition. This could lead to remote information disclosure with System execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142544793 **CVE ID : CVE-2020-0141**		
Information Exposure	11-06-2020	5	In rw_i93_sm_format of rw_i93.c, there is a possible information disclosure due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-146435761 **CVE ID : CVE-2020-0142**	N/A	O-GOO-ANDR-060820/1348
Out-of-bounds Read	11-06-2020	2.1	In nfa_dm_ndef_find_next_handler of nfa_dm_ndef.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure of heap data via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145597277	N/A	O-GOO-ANDR-060820/1349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0143		
Out-of-bounds Read	11-06-2020	2.1	In btm_proc_sp_req_evt of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142543497 **CVE ID : CVE-2020-0144**	N/A	O-GOO-ANDR-060820/1350
Out-of-bounds Read	11-06-2020	2.1	In btm_simple_pair_complete of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142544079 **CVE ID : CVE-2020-0145**	N/A	O-GOO-ANDR-060820/1351
Out-of-bounds Read	11-06-2020	2.1	In btu_hcif_hardware_error_evt of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure via compromised device	N/A	O-GOO-ANDR-060820/1352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142546561 **CVE ID : CVE-2020-0146**		
Out-of-bounds Read	11-06-2020	2.1	In btu_hcif_esco_connection_chg_evt of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142638392 **CVE ID : CVE-2020-0147**	N/A	O-GOO-ANDR-060820/1353
Out-of-bounds Read	11-06-2020	2.1	In btu_hcif_pin_code_request_evt, btu_hcif_link_key_request_evt, and btu_hcif_link_key_notification_evt of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure via compromised device firmware with System execution privileges needed. User interaction is not needed for	N/A	O-GOO-ANDR-060820/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10Android ID: A-142638492 **CVE ID : CVE-2020-0148**		
Out-of-bounds Read	11-06-2020	2.1	In btu_hcif_mode_change_evt of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142544089 **CVE ID : CVE-2020-0149**	N/A	O-GOO-ANDR-060820/1355
Out-of-bounds Write	11-06-2020	4.6	In rw_t3t_message_set_block_list of rw_t3t.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142280329 **CVE ID : CVE-2020-0150**	N/A	O-GOO-ANDR-060820/1356
Out-of-bounds Read	11-06-2020	2.1	In avb_vbmeta_image_verify of avb_vbmeta_image.c there is a possible out of bounds read due to a missing bounds check. This could lead to a local information	N/A	O-GOO-ANDR-060820/1357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-133164384 **CVE ID : CVE-2020-0151**		
Out-of-bounds Read	11-06-2020	2.1	In avb_vbmeta_image_verify of avb_vbmeta_image.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145992159 **CVE ID : CVE-2020-0152**	N/A	O-GOO-ANDR-060820/1358
Out-of-bounds Write	11-06-2020	4.6	In phNxpNciHal_write_ext of phNxpNciHal_ext.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139733543 **CVE ID : CVE-2020-0153**	N/A	O-GOO-ANDR-060820/1359
Out-of-bounds Read	11-06-2020	2.1	In nci_proc_core_rsp of nci_hrcv.cc, there is a possible out of bounds read	N/A	O-GOO-ANDR-060820/1360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to an incorrect bounds check. This could lead to local information disclosure via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141550919 **CVE ID : CVE-2020-0154**		
Out-of-bounds Write	11-06-2020	4.6	In phNxpNciHal_send_ese_hal_cmd of phNxpNciHal_ext.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139736386 **CVE ID : CVE-2020-0155**	N/A	O-GOO-ANDR-060820/1361
Out-of-bounds Read	11-06-2020	2.1	In NxpNfc::ioctl of NxpNfc.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139736127	N/A	O-GOO-ANDR-060820/1362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0156		
Use After Free	10-06-2020	4.9	In sendCaptureResult of Camera3OutputUtils.cpp, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-9Android ID: A-150944913 **CVE ID : CVE-2020-0113**	N/A	O-GOO-ANDR-060820/1363
Improper Privilege Management	10-06-2020	7.2	In onCreateSliceProvider of KeyguardSliceProvider.java, there is a possible confused deputy due to a PendingIntent error. This could lead to local escalation of privilege that allows actions performed as the System UI, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-147606347 **CVE ID : CVE-2020-0114**	N/A	O-GOO-ANDR-060820/1364
Improper Privilege Management	10-06-2020	7.2	In verifyIntentFiltersIfNeeded of PackageManagerService.java , there is a possible settings bypass allowing an app to become the default handler for arbitrary domains. This could lead to local escalation	N/A	O-GOO-ANDR-060820/1365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-8.0Android ID: A-150038428 **CVE ID : CVE-2020-0115**		
Incorrect Default Permissions	10-06-2020	4.9	In checkSystemLocationAccess of LocationAccessPolicy.java, there is a possible bypass of user profile isolation due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-151330809 **CVE ID : CVE-2020-0116**	N/A	O-GOO-ANDR-060820/1366
Integer Overflow or Wraparound	10-06-2020	10	In aes_cmac of aes_cmac.cc, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution in the bluetooth server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-8.0Android ID: A-151155194	N/A	O-GOO-ANDR-060820/1367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0117		
Out-of-bounds Write	10-06-2020	6.9	In addListener of RegionSamplingThread.cpp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-150904694 **CVE ID : CVE-2020-0118**	N/A	O-GOO-ANDR-060820/1368
Improper Certificate Validation	10-06-2020	5.4	In addOrUpdateNetworkInternal and related functions of WifiConfigManager.java, there is a possible man in the middle attack due to improper certificate validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-150500247 **CVE ID : CVE-2020-0119**	N/A	O-GOO-ANDR-060820/1369
Incorrect Default Permissions	10-06-2020	2.1	In updateUidProcState of AppOpsService.java, there is a possible permission bypass due to a logic error. This could lead to local information disclosure of location data with User execution privileges needed. User interaction is not	N/A	O-GOO-ANDR-060820/1370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-148180766 **CVE ID : CVE-2020-0121**		
Out-of-bounds Write	11-06-2020	4.6	In markBootComplete of InstalldNativeService.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140237592 **CVE ID : CVE-2020-0124**	N/A	O-GOO-ANDR-060820/1371
Use After Free	11-06-2020	6.9	In multiple functions in DrmPlugin.cpp, there is a possible use after free due to a race condition. This could lead to local code execution with System execution privileges required. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-137878930 **CVE ID : CVE-2020-0126**	N/A	O-GOO-ANDR-060820/1372
Out-of-bounds Read	11-06-2020	4.3	In AudioStream::decode of AudioGroup.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure in the phone process with no additional	N/A	O-GOO-ANDR-060820/1373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140054506 **CVE ID : CVE-2020-0127**		
Integer Overflow or Wraparound	11-06-2020	5	In addPacket of AMPEG4ElementaryAssembler, there is an out of bounds read due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges required. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-123940919 **CVE ID : CVE-2020-0128**	N/A	O-GOO-ANDR-060820/1374
Out-of-bounds Write	11-06-2020	4.6	In SetData of btm_ble_multi_adv.cc, there is a possible out-of-bound write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-123292010 **CVE ID : CVE-2020-0129**	N/A	O-GOO-ANDR-060820/1375
Out-of-bounds Write	11-06-2020	6.8	In parseChunk of MPEG4Extractor.cpp, there is a possible out of bounds write due to incompletely initialized data. This could	N/A	O-GOO-ANDR-060820/1376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-151159638 **CVE ID : CVE-2020-0131**		
Out-of-bounds Read	11-06-2020	4	In nfa_hci_conn_cback of nfa_hci_main.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139740814 **CVE ID : CVE-2020-0157**	N/A	O-GOO-ANDR-060820/1377
Out-of-bounds Read	11-06-2020	2.1	In nfc_ncif_proc_t3t_polling_ntf of nfc_ncif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141547128 **CVE ID : CVE-2020-0158**	N/A	O-GOO-ANDR-060820/1378
Out-of-bounds Read	11-06-2020	3.5	In rw_mfc_writeBlock of rw_mfc.cc, there is a possible	N/A	O-GOO-ANDR-060820/1379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140768035 **CVE ID : CVE-2020-0159**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-06-2020	6.8	In setSyncSampleParams of SampleTable.cpp, there is possible resource exhaustion due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-124771364 **CVE ID : CVE-2020-0160**	N/A	O-GOO-ANDR-060820/1380
Improper Input Validation	11-06-2020	4.3	In parseChunk of MPEG4Extractor.cpp, there is possible resource exhaustion due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127973550 **CVE ID : CVE-2020-0161**	N/A	O-GOO-ANDR-060820/1381
Improper Input	11-06-2020	4.3	In parseSampleAuxiliaryInform	N/A	O-GOO-ANDR-060820/1382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			ationOffsets of MPEG4Extractor.cpp, there is possible resource exhaustion due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-124526959 **CVE ID : CVE-2020-0162**		
Improper Input Validation	11-06-2020	4.3	In parseSampleAuxiliaryInformationSizes of MPEG4Extractor.cpp, there is possible resource exhaustion due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-124525515 **CVE ID : CVE-2020-0163**	N/A	O-GOO-ANDR-060820/1383
Out-of-bounds Read	11-06-2020	2.1	In phNxpNciHal_NfcDep_cmd_ext of phNxpNciHal_NfcDepSWPrio.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	N/A	O-GOO-ANDR-060820/1384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10Android ID: A-139736125 **CVE ID : CVE-2020-0164**		
Out-of-bounds Write	11-06-2020	7.2	In phNxpNciHal_NfcDep_cmd_ext of phNxpNciHal_NfcDepSWPrio.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139532977 **CVE ID : CVE-2020-0165**	N/A	O-GOO-ANDR-060820/1385
Improper Privilege Management	11-06-2020	4.6	In multiple functions of URI.java, there is a possible escalation of privilege due to missing validation in the parceling of URI information. This could lead to a local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-124526860 **CVE ID : CVE-2020-0166**	N/A	O-GOO-ANDR-060820/1386
Out-of-bounds Read	11-06-2020	4.3	In load of ResourceTypes.cpp, there is a possible out of bounds read due to an integer	N/A	O-GOO-ANDR-060820/1387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-129475100 **CVE ID : CVE-2020-0167**		
Out-of-bounds Write	11-06-2020	6.8	In impeg2_fmt_conv_yuv420p_to_yuv420sp_uv of impeg2_format_conv.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-137798382 **CVE ID : CVE-2020-0168**	N/A	O-GOO-ANDR-060820/1388
Uncontrolled Resource Consumption	11-06-2020	4.3	In RTTTL_Event of eas_rtttl.c, there is possible resource exhaustion due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-123700383 **CVE ID : CVE-2020-0169**	N/A	O-GOO-ANDR-060820/1389
Uncontrolled Resource Consumption	11-06-2020	4.3	In IMY_Event of eas_imelody.c, there is possible resource exhaustion	N/A	O-GOO-ANDR-060820/1390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127310810 **CVE ID : CVE-2020-0170**		
Uncontrolled Resource Consumption	11-06-2020	4.3	In Parse_lart of eas_mdls.c, there is possible resource exhaustion due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127313223 **CVE ID : CVE-2020-0171**	N/A	O-GOO-ANDR-060820/1391
Uncontrolled Resource Consumption	11-06-2020	4.3	In Parse_art of eas_mdls.c, there is possible resource exhaustion due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127312550 **CVE ID : CVE-2020-0172**	N/A	O-GOO-ANDR-060820/1392
Uncontrolled Resource Consumption	11-06-2020	4.3	In Parse_lins of eas_mdls.c, there is possible resource exhaustion due to improper input validation. This could lead to remote denial of	N/A	O-GOO-ANDR-060820/1393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127313764 **CVE ID : CVE-2020-0173**		
Uncontrolled Resource Consumption	11-06-2020	4.3	In Parse_ptbl of eas_mdls.c, there is possible resource exhaustion due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127313537 **CVE ID : CVE-2020-0174**	N/A	O-GOO-ANDR-060820/1394
Uncontrolled Resource Consumption	11-06-2020	4.3	In XMF_ReadNode of eas_xmf.c, there is possible resource exhaustion due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-126380818 **CVE ID : CVE-2020-0175**	N/A	O-GOO-ANDR-060820/1395
Out-of-bounds Read	11-06-2020	5	In avdt_msg_prs_rej of avdt_msg.cc, there is a possible out-of-bounds read due to improper input validation. This could lead to remote information disclosure with no additional	N/A	O-GOO-ANDR-060820/1396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-79702484 **CVE ID : CVE-2020-0176**		
Improper Privilege Management	11-06-2020	2.1	In connect() of PanService.java, there is a possible permissions bypass. This could lead to local escalation of privilege to change network connection settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-126206353 **CVE ID : CVE-2020-0177**	N/A	O-GOO-ANDR-060820/1397
Information Exposure	11-06-2020	2.1	In getAllConfigFlags of SettingsProvider.cpp, there is a possible illegal read due to a missing permission check. This could lead to local information disclosure of config flags with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143299398 **CVE ID : CVE-2020-0178**	N/A	O-GOO-ANDR-060820/1398
Improper Input Validation	11-06-2020	6.8	In doSendObjectInfo of MtpServer.cpp, there is a possible path traversal attack due to insufficient	N/A	O-GOO-ANDR-060820/1399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is required for exploitation.Product: AndroidVersions: Android-10Android ID: A-130656917 **CVE ID : CVE-2020-0179**		
Time-of-check Time-of-use (TOCTOU) Race Condition	11-06-2020	5.1	In InstallPackage of package.cpp, there is a possible bypass of a signature check due to a Time of Check/Time of Use condition. This could lead to local escalation of privilege by allowing a bypass of the initial zip file signature check for an OS update with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-136498130 **CVE ID : CVE-2020-0204**	N/A	O-GOO-ANDR-060820/1400
Out-of-bounds Read	11-06-2020	4.3	In the DaalaBitReader constructor of entropy_decoder.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure in the media server with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-147234020	N/A	O-GOO-ANDR-060820/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0205		
Improper Input Validation	11-06-2020	2.1	In the settings app, there is a possible app crash due to improper input validation. This could lead to local denial of service of the Settings app with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-136005061 **CVE ID : CVE-2020-0206**	N/A	O-GOO-ANDR-060820/1402
Out-of-bounds Read	11-06-2020	4.3	In next_marker of jdmarker.c, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-135532289 **CVE ID : CVE-2020-0207**	N/A	O-GOO-ANDR-060820/1403
Incorrect Default Permissions	11-06-2020	4.6	In multiple functions of AccountManager.java, there is a possible permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145207098 **CVE ID : CVE-2020-0208**	N/A	O-GOO-ANDR-060820/1404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	11-06-2020	4.6	In multiple functions of AccountManager.java, there is a possible permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145206842 **CVE ID : CVE-2020-0209**	N/A	O-GOO-ANDR-060820/1405
Externally Controlled Reference to a Resource in Another Sphere	11-06-2020	4.6	In removeSharedAccountAsUser of AccountManager.java, there is a possible permissions bypass to a confused deputy. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145206763 **CVE ID : CVE-2020-0210**	N/A	O-GOO-ANDR-060820/1406
Out-of-bounds Read	11-06-2020	4.3	In SumCompoundHorizontalTaps of convolve_neon.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-147491773	N/A	O-GOO-ANDR-060820/1407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0211		
Use After Free	11-06-2020	4.3	In _onBufferDestroyed of InputBufferManager.cpp, there is a possible out of bounds read due to a use after free. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-135140854 **CVE ID : CVE-2020-0212**	N/A	O-GOO-ANDR-060820/1408
Out-of-bounds Write	11-06-2020	6.8	In hevcd_fmt_conv_420sp_to_420sp_av8 of ihevcd_fmt_conv_420sp_to_420sp.s, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143464314 **CVE ID : CVE-2020-0213**	N/A	O-GOO-ANDR-060820/1409
Out-of-bounds Read	11-06-2020	5	In ce_t4t_process_select_file_cmd of ce_t4t.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for	N/A	O-GOO-ANDR-060820/1410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10Android ID: A-140292264 **CVE ID : CVE-2020-0214**		
Incorrect Default Permissions	11-06-2020	4.4	In onCreate of ConfirmConnectActivity.java, there is a possible leak of Bluetooth information due to a permissions bypass. This could lead to local escalation of privilege of a pairing Bluetooth MAC address with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140417248 **CVE ID : CVE-2020-0215**	N/A	O-GOO-ANDR-060820/1411
Integer Overflow or Wraparound	11-06-2020	4.4	In phNciNfc_RecvMfResp of phNxpExtns_MifareStd.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-126204073 **CVE ID : CVE-2020-0216**	N/A	O-GOO-ANDR-060820/1412
Out-of-bounds Write	11-06-2020	7.5	In RW_T4tPresenceCheck of rw_t4t.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed.	N/A	O-GOO-ANDR-060820/1413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141331405 **CVE ID : CVE-2020-0217**		
Out-of-bounds Write	11-06-2020	4.4	In loadSoundModel and related functions of SoundTriggerHwService.cpp, there is possible out of bounds write due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-136005905 **CVE ID : CVE-2020-0218**	N/A	O-GOO-ANDR-060820/1414
Improper Privilege Management	11-06-2020	4.6	In onCreate of SliceDeepLinkSpringBoard.java there is a possible insecure Intent. This could lead to local elevation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-122836081 **CVE ID : CVE-2020-0219**	N/A	O-GOO-ANDR-060820/1415
Use After Free	11-06-2020	7.2	In main of main.cpp, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution	N/A	O-GOO-ANDR-060820/1416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-150225255 **CVE ID : CVE-2020-0233**		
N/A	04-06-2020	5	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Attackers can disable the SEAndroid protection mechanism in the RKP. The Samsung ID is SVE-2019-15998 (June 2020). **CVE ID : CVE-2020-13829**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-060820/1417
Information Exposure	04-06-2020	5	An issue was discovered on Samsung mobile devices with P(9.0) software. One UI HOME logging can leak information. The Samsung ID is SVE-2019-16382 (June 2020). **CVE ID : CVE-2020-13830**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-060820/1418
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-06-2020	7.5	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (Exynos 7570 chipsets) software. The Trustonic Kinibi component allows arbitrary memory mapping. The Samsung ID is SVE-2019-16665 (June 2020). **CVE ID : CVE-2020-13831**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-060820/1419
Improper Restriction of Operations within the	04-06-2020	7.5	An issue was discovered on Samsung mobile devices with Q(10.0) (with TEEGRIS on Exynos chipsets) software. The Widevine	https://security.samsungmobile.com/securityUpdate.sms	O-GOO-ANDR-060820/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Trustlet allows arbitrary code execution because of memory disclosure, The Samsung IDs are SVE-2020-17117, SVE-2020-17118, SVE-2020-17119, and SVE-2020-17161 (June 2020). **CVE ID : CVE-2020-13832**	b	
Improper Link Resolution Before File Access ('Link Following')	04-06-2020	6.4	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. The system area allows arbitrary file overwrites via a symlink attack. The Samsung ID is SVE-2020-17183 (June 2020). **CVE ID : CVE-2020-13833**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-060820/1421
Incorrect Authorization	04-06-2020	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (with TEEGRIS) software. Secure Folder does not properly restrict use of Android Debug Bridge (adb) for arbitrary installations. The Samsung ID is SVE-2020-17369 (June 2020). **CVE ID : CVE-2020-13834**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-060820/1422
Insufficiently Protected Credentials	04-06-2020	5	An issue was discovered on Samsung mobile devices with O(8.x) (with TEEGRIS) software. The Gatekeeper Trustlet allows a brute-force attack on user credentials. The Samsung ID is SVE-2020-16908 (June 2020). **CVE ID : CVE-2020-13835**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-060820/1423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-06-2020	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. HWRResProvider allows path traversal for data exposure. The Samsung ID is SVE-2020-16954 (June 2020). **CVE ID : CVE-2020-13836**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-060820/1424
Improper Authentication	04-06-2020	3.6	An issue was discovered on Samsung mobile devices with Q(10.0) software. The Lockscreen feature does not block Quick Panel access to Music Share. The Samsung ID is SVE-2020-17145 (June 2020). **CVE ID : CVE-2020-13837**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-060820/1425
Improper Authentication	04-06-2020	3.6	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. The DeX Lockscreen feature does not block access to Quick Panel and notifications. The Samsung ID is SVE-2020-17187 (June 2020). **CVE ID : CVE-2020-13838**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-060820/1426
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	O-GOO-ANDR-060820/1427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	O-GOO-ANDR-060820/1428
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	O-GOO-ANDR-060820/1429
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	O-GOO-ANDR-060820/1430
Improper Input Validation	05-06-2020	4.9	An issue was discovered on LG mobile devices with Android OS software before 2020-06-01. Local users can cause a denial of service because checking of the userdata partition is mishandled. The LG ID is LVE-SMP-200014 (June	https://lgsecurity.lge.com/	O-GOO-ANDR-060820/1431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020). **CVE ID : CVE-2020-13843**		
Improper Input Validation	03-06-2020	4.3	Incorrect security UI in payments in Google Chrome on Android prior to 83.0.4103.97 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2020-6494**	N/A	O-GOO-ANDR-060820/1432
homey					
homey_firmware					
Cleartext Storage of Sensitive Information	04-06-2020	3.3	An issue was discovered in all Athom Homey and Homey Pro devices up to the current version 4.2.0. An attacker within RF range can obtain a cleartext copy of the network configuration of the device, including the Wi-Fi PSK, during device setup. Upon success, the attacker is able to further infiltrate the target's Wi-Fi networks. **CVE ID : CVE-2020-9462**	N/A	O-HOM-HOME-060820/1433
homey_pro_firmware					
Cleartext Storage of Sensitive Information	04-06-2020	3.3	An issue was discovered in all Athom Homey and Homey Pro devices up to the current version 4.2.0. An attacker within RF range can obtain a cleartext copy of the network configuration of the device, including the Wi-Fi PSK, during device setup. Upon success, the attacker is able to further infiltrate the	N/A	O-HOM-HOME-060820/1434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			target's Wi-Fi networks. **CVE ID : CVE-2020-9462**		
HP					
x3220nr_firmware					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	O-HP-X322-060820/1435
Huawei					
honor_view_20_firmware					
Improper Handling of Exceptional Conditions	05-06-2020	5	Huawei Smartphones HONOR 20 PRO;Honor View 20;HONOR 20 have an improper handling of exceptional condition Vulnerability. A component cannot deal with an exception correctly. Attackers can exploit this vulnerability by sending malformed message. This could compromise normal service of affected phones. **CVE ID : CVE-2020-9074**	N/A	O-HUA-HONO-060820/1436
honor_20_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	05-06-2020	5	Huawei Smartphones HONOR 20 PRO;Honor View 20;HONOR 20 have an improper handling of exceptional condition Vulnerability. A component cannot deal with an exception correctly. Attackers can exploit this vulnerability by sending malformed message. This could compromise normal service of affected phones. **CVE ID : CVE-2020-9074**	N/A	O-HUA-HONO-060820/1437
honor_20_pro_firmware					
Improper Handling of Exceptional Conditions	05-06-2020	5	Huawei Smartphones HONOR 20 PRO;Honor View 20;HONOR 20 have an improper handling of exceptional condition Vulnerability. A component cannot deal with an exception correctly. Attackers can exploit this vulnerability by sending malformed message. This could compromise normal service of affected phones. **CVE ID : CVE-2020-9074**	N/A	O-HUA-HONO-060820/1438
ar1200-s_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending	N/A	O-HUA-AR12-060820/1439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**		
ar1200_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	O-HUA-AR12-060820/1440
ar150_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the	N/A	O-HUA-AR15-060820/1441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**		
ar160_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	O-HUA-AR16-060820/1442
ar200_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit	N/A	O-HUA-AR20-060820/1443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200 R007C00SPCa00 **CVE ID : CVE-2020-9071**		
ar2200_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200 R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	O-HUA-AR22-060820/1444
ar3200_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal	N/A	O-HUA-AR32-060820/1445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**		
srg1300_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	O-HUA-SRG1-060820/1446
srg2300_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected	N/A	O-HUA-SRG2-060820/1447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**		
srg3300_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	O-HUA-SRG3-060820/1448
ar510_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions	N/A	O-HUA-AR51-060820/1449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**		
usg6300e_firmware					
Information Exposure	15-06-2020	4	Huawei products Secospace USG6300;USG6300E with versions of V500R001C30,V500R001C50,V500R001C60,V500R001C80,V500R005C00,V500R005C10;V600R006C00 have a vulnerability of insufficient input verification. An attacker with limited privilege can exploit this vulnerability to access a specific directory. Successful exploitation of this vulnerability may lead to information leakage. **CVE ID : CVE-2020-9075**	N/A	O-HUA-USG6-060820/1450
ips_module_firmware					
Improper Authentication	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20;	N/A	O-HUA-IPS_-060820/1451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**		
ar120-s_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	O-HUA-AR12-060820/1452
tony-al00b_firmware					
Improper Authentication	15-06-2020	4	HUAWEI P30;HUAWEI P30 Pro;Tony-AL00B smartphones with versions earlier than 10.1.0.135(C00E135R2P11); versions earlier than 10.1.0.135(C00E135R2P8),	N/A	O-HUA-TONY-060820/1453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions earlier than 10.1.0.135 have an improper authentication vulnerability. Due to the identity of the message sender not being properly verified, an attacker can exploit this vulnerability through man-in-the-middle attack to induce user to access malicious URL. **CVE ID : CVE-2020-9076**		
nip6300_firmware					
Improper Authentication	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device.	N/A	O-HUA-NIP6-060820/1454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9099		
nip6600_firmware					
Improper Authenticati on	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**	N/A	O-HUA-NIP6-060820/1455
nip6800_firmware					
Missing Release of Resource after Effective Lifetime	05-06-2020	4	Huawei products NIP6800;Secospace USG6600;USG9500 have a memory leak vulnerability. An attacker with high privileges exploits this vulnerability by continuously performing specific operations.	N/A	O-HUA-NIP6-060820/1456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability can cause service abnormal. **CVE ID : CVE-2020-1883**		
Improper Authentication	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**	N/A	O-HUA-NIP6-060820/1457
secospace_usg6300_firmware					
Information Exposure	15-06-2020	4	Huawei products Secospace USG6300;USG6300E with versions of V500R001C30,V500R001C50,V500R001C60,V500R001C80,V500R005C00,V500R005C10;V600R006C00 have a	N/A	O-HUA-SECO-060820/1458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability of insufficient input verification. An attacker with limited privilege can exploit this vulnerability to access a specific directory. Successful exploitation of this vulnerability may lead to information leakage. **CVE ID : CVE-2020-9075**		
Improper Authentication	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**	N/A	O-HUA-SECO-060820/1459
secospace_usg6500_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authenticati on	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**	N/A	O-HUA-SECO-060820/1460
secospace_usg6600_firmware					
Missing Release of Resource after Effective Lifetime	05-06-2020	4	Huawei products NIP6800;Secospace USG6600;USG9500 have a memory leak vulnerability. An attacker with high privileges exploits this vulnerability by continuously performing specific operations. Successful exploitation of this vulnerability can cause	N/A	O-HUA-SECO-060820/1461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service abnormal. **CVE ID : CVE-2020-1883**		
Information Exposure	15-06-2020	4	Huawei products Secospace USG6300;USG6300E with versions of V500R001C30,V500R001C50,V500R001C60,V500R001C80,V500R005C00,V500R005C10;V600R006C00 have a vulnerability of insufficient input verification. An attacker with limited privilege can exploit this vulnerability to access a specific directory. Successful exploitation of this vulnerability may lead to information leakage. **CVE ID : CVE-2020-9075**	N/A	O-HUA-SECO-060820/1462
Improper Authentication	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication	N/A	O-HUA-SECO-060820/1463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**		
p30_pro_firmware					
Improper Authentication	15-06-2020	4	HUAWEI P30;HUAWEI P30 Pro;Tony-AL00B smartphones with versions earlier than 10.1.0.135(C00E135R2P11); versions earlier than 10.1.0.135(C00E135R2P8), versions earlier than 10.1.0.135 have an improper authentication vulnerability. Due to the identity of the message sender not being properly verified, an attacker can exploit this vulnerability through man-in-the-middle attack to induce user to access malicious URL. **CVE ID : CVE-2020-9076**	N/A	O-HUA-P30_-060820/1464
p30_firmware					
Improper Authentication	15-06-2020	4	HUAWEI P30;HUAWEI P30 Pro;Tony-AL00B smartphones with versions earlier than 10.1.0.135(C00E135R2P11); versions earlier than 10.1.0.135(C00E135R2P8), versions earlier than 10.1.0.135 have an improper authentication vulnerability. Due to the identity of the	N/A	O-HUA-P30_-060820/1465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			message sender not being properly verified, an attacker can exploit this vulnerability through man-in-the-middle attack to induce user to access malicious URL. **CVE ID : CVE-2020-9076**		
Improper Authentication	15-06-2020	4.6	HUAWEI P30 smart phone with versions earlier than 10.1.0.135(C00E135R2P11) have an improper authentication vulnerability. Due to improper authentication of specific interface, in specific scenario attackers could access specific interface without authentication. Successful exploit could allow the attacker to perform unauthorized operations. **CVE ID : CVE-2020-1813**	N/A	O-HUA-P30_-060820/1466
ar150-s_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200	N/A	O-HUA-AR15-060820/1467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R007C00SPCa00 **CVE ID : CVE-2020-9071**		
ar200-s_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	O-HUA-AR20-060820/1468
ar2200-s_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00	N/A	O-HUA-AR22-060820/1469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9071		
ar3600_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	O-HUA-AR36-060820/1470
netengine16ex_firmware					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	O-HUA-NETE-060820/1471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ngfw_module_firmware					
Improper Authenticati on	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**	N/A	O-HUA-NGFW-060820/1472
usg9500_firmware					
Missing Release of Resource after Effective Lifetime	05-06-2020	4	Huawei products NIP6800;Secospace USG6600;USG9500 have a memory leak vulnerability. An attacker with high privileges exploits this vulnerability by continuously performing specific operations. Successful exploitation of	N/A	O-HUA-USG9-060820/1473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can cause service abnormal. **CVE ID : CVE-2020-1883**		
Improper Authenticati on	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**	N/A	O-HUA-USG9-060820/1474
IBM					
AIX					
Improper Restriction of Rendered UI Layers or Frames	15-06-2020	3.5	IBM Spectrum Protect Client 8.1.7.0 through 8.1.9.1 (Linux and Windows), 8.1.9.0 trough 8.1.9.1 (AIX) and IBM Spectrum Protect for Space Management	https://www.ibm.com/support/pages/node/6221448	O-IBM-AIX-060820/1475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.1.7.0 through 8.1.9.1 (Linux), 8.1.9.0 through 8.1.9.1 (AIX) web user interfaces could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 179488. **CVE ID : CVE-2020-4406**		
Information Exposure	15-06-2020	5	IBM Spectrum Protect Client 8.1.7.0 through 8.1.9.1 (Linux and Windows), 8.1.9.0 trough 8.1.9.1 (AIX) and IBM Spectrum Protect for Space Management 8.1.7.0 through 8.1.9.1 (Linux), 8.1.9.0 through 8.1.9.1 (AIX) web user interfaces could allow an attacker to bypass authentication due to improper session validation which can result in access to unauthorized resources. IBM X-Force ID: 182019. **CVE ID : CVE-2020-4494**	https://www.ibm.com/support/pages/node/6221448	O-IBM-AIX-060820/1476
i					
Missing Authorization	09-06-2020	9.3	The file transfer component of TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for IBM i contains a vulnerability that	https://www.tibco.com/services/support/advisories, https://ww	O-IBM-I-060820/1477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			theoretically allows an attacker to perform unauthorized network file transfers to and from the file system accessible to the affected component. This vulnerability is exploitable when the configuration option 'Require Node Resp' is set to 'No'. In the event of a successful exploit, the attacker could theoretically read and write any file on the file system accessible to the affected component, thus fully affecting the confidentiality, integrity, and availability of the operating system hosting the deployment of the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for IBM i: versions 7.1.0 and below, version 8.0.0. **CVE ID : CVE-2020-9411**	w.tibco.com /support/advisories/2020/06/tibco-security-advisory-june-9-2020-tibco-managed-file-transfer-2020-9411	
Improper Input Validation	09-06-2020	10	The file transfer component of TIBCO Software Inc.'s TIBCO Managed File Transfer Platform Server for IBM i contains a vulnerability that theoretically allows execution of arbitrary commands at the privilege level of the affected system following a failed file transfer. Affected releases are TIBCO Software Inc.'s TIBCO Managed File	https://www.tibco.com /services/support/advisories, https://www.tibco.com /support/advisories/2020/06/tibco-security-advisory-june-9-2020-tibco-	O-IBM-I-060820/1478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Transfer Platform Server for IBM i: versions 7.1.0 and below, version 8.0.0. **CVE ID : CVE-2020-9412**	managed-file-transfer-2020-9412	
Intel					
active_management_technology_firmware					
Out-of-bounds Read	15-06-2020	7.5	Out-of-bounds read in IPv6 subsystem in Intel(R) AMT and Intel(R) ISM versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable escalation of privilege via network access. **CVE ID : CVE-2020-0594**	https://www.synology.com/security/advisory/Synology_SA_20_15	O-INT-ACTI-060820/1479
Use After Free	15-06-2020	7.5	Use after free in IPv6 subsystem in Intel(R) AMT and Intel(R) ISM versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable escalation of privilege via network access. **CVE ID : CVE-2020-0595**	https://www.synology.com/security/advisory/Synology_SA_20_15	O-INT-ACTI-060820/1480
Improper Input Validation	15-06-2020	5	Improper input validation in DHCPv6 subsystem in Intel(R) AMT and Intel(R) ISM versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable information disclosure via network access. **CVE ID : CVE-2020-0596**	https://www.synology.com/security/advisory/Synology_SA_20_15	O-INT-ACTI-060820/1481
Improper	15-06-2020	4	Improper input validation in	N/A	O-INT-ACTI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Intel(R) AMT versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an authenticated user to potentially enable information disclosure via network access. **CVE ID : CVE-2020-0531**		060820/1482
Improper Input Validation	15-06-2020	4.8	Improper input validation in subsystem for Intel(R) AMT versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2020-0532**	N/A	O-INT-ACTI-060820/1483
Improper Input Validation	15-06-2020	5	Improper input validation in Intel(R) AMT versions before 11.8.76, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable information disclosure via network access. **CVE ID : CVE-2020-0535**	N/A	O-INT-ACTI-060820/1484
Improper Input Validation	15-06-2020	4	Improper input validation in subsystem for Intel(R) AMT versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow a privileged user to potentially enable denial of service via network access. **CVE ID : CVE-2020-0537**	N/A	O-INT-ACTI-060820/1485
Improper Input	15-06-2020	5	Improper input validation in subsystem for Intel(R) AMT	N/A	O-INT-ACTI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable denial of service via network access. **CVE ID : CVE-2020-0538**		060820/1486
Insufficiently Protected Credentials	15-06-2020	5	Insufficiently protected credentials in Intel(R) AMT versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable information disclosure via network access. **CVE ID : CVE-2020-0540**	N/A	O-INT-ACTI-060820/1487
Out-of-bounds Read	15-06-2020	5	Out-of-bounds read in DHCPv6 subsystem in Intel(R) AMT and Intel(R)ISM versions before 11.8.77, 11.12.77, 11.22.77, 12.0.64 and 14.0.33 may allow an unauthenticated user to potentially enable information disclosure via network access. **CVE ID : CVE-2020-8674**	https://www.synology.com/security/advisory/Synology_SA_20_15	O-INT-ACTI-060820/1488
core_i7-10700f_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access.	N/A	O-INT-CORE-060820/1489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0528		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1490
core_i7-10700e_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1491
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1492
core_i7-10700_firmware					
Improper Restriction of Operations within the Bounds of a Memory	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation	N/A	O-INT-CORE-060820/1493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1494
core_i7-10610u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1495
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1496
core_i7-1060g7_firmware					
Improper Restriction of Operations within the	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an	N/A	O-INT-CORE-060820/1497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1498
core_i7-1068ng7_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1499
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1500
core_i7-8665ue_firmware					
Improper Restriction of	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation	N/A	O-INT-CORE-060820/1501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1502
core_i7-8665u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1503
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1504
core_i7-8557u_firmware					
Improper	15-06-2020	4.6	Improper buffer restrictions	N/A	O-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		060820/1505
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1506
core_i7-8850h_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1507
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-8809g_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1509
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1510
core_i7-8750h_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1511
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation	N/A	O-INT-CORE-060820/1512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-8709g_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1513
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1514
core_i7-8706g_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1515
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an	N/A	O-INT-CORE-060820/1516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-8705g_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1517
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1518
core_i7-8700t_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1519
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R)	N/A	O-INT-CORE-060820/1520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-8700k_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1521
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1522
core_i7-8700b_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1523
Improper	15-06-2020	4.6	Improper initialization in	N/A	O-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization			BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		060820/1524
core_i7-8700_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1525
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1526
core_i7\+8700_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access.	N/A	O-INT-CORE-060820/1527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0528		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1528
core_i7-8569u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1529
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1530
core_i7-8650u_firmware					
Improper Restriction of Operations within the Bounds of a Memory	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation	N/A	O-INT-CORE-060820/1531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1532
core_i7-8565u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1533
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1534
core_i7-8559u_firmware					
Improper Restriction of Operations within the	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an	N/A	O-INT-CORE-060820/1535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1536
core_i7-8550u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1537
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1538
core_i7-8500y_firmware					
Improper Restriction of	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation	N/A	O-INT-CORE-060820/1539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1540
core_i7-8086k_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1541
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1542
core_i9-9980hk_firmware					
Improper	15-06-2020	4.6	Improper buffer restrictions	N/A	O-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		060820/1543
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1544
core_i9-9880h_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1545
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i9-9900t_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1547
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1548
core_i9-9900ks_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1549
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation	N/A	O-INT-CORE-060820/1550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i9-9900kf_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1551
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1552
core_i9-9900k_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1553
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an	N/A	O-INT-CORE-060820/1554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i9-9900_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1555
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1556
ssd_d3-s4510_firmware					
Information Exposure	15-06-2020	2.1	Insufficient control flow management in firmware for some Intel(R) Data Center SSDs may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0527**	N/A	O-INT-SSD_-060820/1557
ssd_dc_p4510_firmware					
Information Exposure	15-06-2020	2.1	Insufficient control flow management in firmware for some Intel(R) Data Center SSDs may allow a privileged	N/A	O-INT-SSD_-060820/1558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0527**		
ssd_dc_p4610_firmware					
Information Exposure	15-06-2020	2.1	Insufficient control flow management in firmware for some Intel(R) Data Center SSDs may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0527**	N/A	O-INT-SSD_-060820/1559
core_i5-7600k_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1560
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1561
core_i5-7600t_firmware					
Improper Restriction of Operations	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor	N/A	O-INT-CORE-060820/1562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1563
core_i5-7600_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1564
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1565
core_i5-7500_firmware					
Improper Restriction	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th,	N/A	O-INT-CORE-060820/1566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1567
core_i5-7500t_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1568
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1569
core_i7-1065g7_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1570
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1571
trusted_execution_engine_firmware					
Improper Input Validation	15-06-2020	5	Improper input validation in the DAL subsystem for Intel(R) CSME versions before 11.8.77, 11.12.77, 11.22.77, 12.0.64, 13.0.32,14.0.33 and Intel(R) TXE versions before 3.1.75 and 4.0.25 may allow an unauthenticated user to potentially enable information disclosure via network access. **CVE ID : CVE-2020-0536**	N/A	O-INT-TRUS-060820/1572
Improper Limitation of a Pathname to a Restricted Directory	15-06-2020	2.1	Path traversal in subsystem for Intel(R) DAL software for Intel(R) CSME versions before 11.8.77, 11.12.77, 11.22.77, 12.0.64, 13.0.32, 14.0.33 and Intel(R) TXE	N/A	O-INT-TRUS-060820/1573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			versions before 3.1.75, 4.0.25 may allow an unprivileged user to potentially enable denial of service via local access. **CVE ID : CVE-2020-0539**		
Improper Privilege Management	15-06-2020	4.6	Improper Access Control in subsystem for Intel(R) TXE versions before 3.175 and 4.0.25 may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2020-0566**	N/A	O-INT-TRUS-060820/1574
converged_security_management_engine_firmware					
Use of Password Hash With Insufficient Computational Effort	15-06-2020	4.6	Reversible one-way hash in Intel(R) CSME versions before 11.8.76, 11.12.77 and 11.22.77 may allow a privileged user to potentially enable escalation of privilege, denial of service or information disclosure via local access. **CVE ID : CVE-2020-0533**	N/A	O-INT-CONV-060820/1575
Improper Input Validation	15-06-2020	5	Improper input validation in the DAL subsystem for Intel(R) CSME versions before 12.0.64, 13.0.32, 14.0.33 and 14.5.12 may allow an unauthenticated user to potentially enable denial of service via network access. **CVE ID : CVE-2020-0534**	N/A	O-INT-CONV-060820/1576
Improper Input	15-06-2020	5	Improper input validation in the DAL subsystem for	N/A	O-INT-CONV-060820/1577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) CSME versions before 11.8.77, 11.12.77, 11.22.77, 12.0.64, 13.0.32,14.0.33 and Intel(R) TXE versions before 3.1.75 and 4.0.25 may allow an unauthenticated user to potentially enable information disclosure via network access. **CVE ID : CVE-2020-0536**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-06-2020	2.1	Path traversal in subsystem for Intel(R) DAL software for Intel(R) CSME versions before 11.8.77, 11.12.77, 11.22.77, 12.0.64, 13.0.32, 14.0.33 and Intel(R) TXE versions before 3.1.75, 4.0.25 may allow an unprivileged user to potentially enable denial of service via local access. **CVE ID : CVE-2020-0539**	N/A	O-INT-CONV-060820/1578
Out-of-bounds Write	15-06-2020	4.6	Out-of-bounds write in subsystem for Intel(R) CSME versions before 12.0.64, 13.0.32, 14.0.33 and 14.5.12 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0541**	N/A	O-INT-CONV-060820/1579
Improper Restriction of Operations within the Bounds of a Memory	15-06-2020	4.6	Improper buffer restrictions in subsystem for Intel(R) CSME versions before 12.0.64, 13.0.32, 14.0.33 and 14.5.12 may allow an authenticated user to potentially enable escalation	N/A	O-INT-CONV-060820/1580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			of privilege, information disclosure or denial of service via local access. **CVE ID : CVE-2020-0542**		
Integer Overflow or Wraparound	15-06-2020	2.1	Integer overflow in subsystem for Intel(R) CSME versions before 11.8.77, 11.12.77, 11.22.77 and Intel(R) TXE versions before 3.1.75, 4.0.25 and Intel(R) Server Platform Services (SPS) versions before SPS_E5_04.01.04.380.0, SPS_SoC-X_04.00.04.128.0, SPS_SoC-A_04.00.04.211.0, SPS_E3_04.01.04.109.0, SPS_E3_04.08.04.070.0 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2020-0545**	https://cert-portal.siemens.com/productcert/pdf/ssa-631949.pdf, https://kc.mcafee.com/corporate/index?page=content&id=SB10321	O-INT-CONV-060820/1581
core_i5-7442eq_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1582
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation	N/A	O-INT-CORE-060820/1583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i5-7440hq_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1584
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1585
core_i5-7440eq_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1586
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an	N/A	O-INT-CORE-060820/1587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i5-7400t_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1588
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1589
core_i5-7400_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1590
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R)	N/A	O-INT-CORE-060820/1591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i5-7360u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1592
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1593
core_i5-7300u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1594
Improper	15-06-2020	4.6	Improper initialization in	N/A	O-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization			BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		060820/1595
core_i5-7300hq_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1596
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1597
core_i5-7287u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access.	N/A	O-INT-CORE-060820/1598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0528		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1599
core_i5-7267u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1600
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1601
core_i5-7260u_firmware					
Improper Restriction of Operations within the Bounds of a Memory	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation	N/A	O-INT-CORE-060820/1602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1603
core_i5-7200u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1604
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1605
core_i5-7y54_firmware					
Improper Restriction of Operations within the	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an	N/A	O-INT-CORE-060820/1606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1607
core_i5-7y57_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1608
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1609
core_i7-7920hq_firmware					
Improper Restriction of	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation	N/A	O-INT-CORE-060820/1610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1611
core_i7-7820hq_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1612
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1613
core_i7-7820hk_firmware					
Improper	15-06-2020	4.6	Improper buffer restrictions	N/A	O-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		060820/1614
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1615
core_i7-7820eq_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1616
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-7700hq_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1618
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1619
core_i7-7700k_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1620
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation	N/A	O-INT-CORE-060820/1621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-7700t_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1622
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1623
core_i7-7660u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1624
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an	N/A	O-INT-CORE-060820/1625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-7600u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1626
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1627
core_i7-7567u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1628
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R)	N/A	O-INT-CORE-060820/1629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-7560u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1630
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1631
core_i7-7500u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1632
Improper	15-06-2020	4.6	Improper initialization in	N/A	O-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization			BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		060820/1633
core_i7-7y75_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1634
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1635
core_i7-10510u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access.	N/A	O-INT-CORE-060820/1636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0528		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1637
core_i7-10510y_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1638
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1639
innovation_engine_firmware					
Improper Privilege Management	15-06-2020	4.6	Insufficient control flow management in firmware build and signing tool for Intel(R) Innovation Engine before version 1.0.859 may allow an unauthenticated user to potentially enable	N/A	O-INT-INNO-060820/1640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege via physical access. **CVE ID : CVE-2020-8675**		
core_i7-10875h_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1641
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1642
core_i7-10850h_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1643
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families	N/A	O-INT-CORE-060820/1644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-10810u_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1645
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1646
core_i7-10750h_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1647
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th	N/A	O-INT-CORE-060820/1648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-10700te_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1649
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1650
core_i7-10700t_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1652
core_i7-10700kf_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1653
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1654
core_i7-10700k_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of	N/A	O-INT-CORE-060820/1655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1656
core_i7-7700_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	O-INT-CORE-060820/1657
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1658
core_i7-10710u_firmware					
Improper Restriction of Operations within the Bounds of a	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to	N/A	O-INT-CORE-060820/1659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	O-INT-CORE-060820/1660
ssd_dc_p4618_firmware					
Information Exposure	15-06-2020	2.1	Insufficient control flow management in firmware for some Intel(R) Data Center SSDs may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0527**	N/A	O-INT-SSD_-060820/1661
ssd_dc_p4511_firmware					
Information Exposure	15-06-2020	2.1	Insufficient control flow management in firmware for some Intel(R) Data Center SSDs may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0527**	N/A	O-INT-SSD_-060820/1662
trusted_execution_engine					
Integer Overflow or Wraparound	15-06-2020	2.1	Integer overflow in subsystem for Intel(R) CSME versions before 11.8.77, 11.12.77, 11.22.77 and Intel(R) TXE versions before 3.1.75, 4.0.25 and Intel(R)	https://cert-portal.siemens.com/productcert/pdf/ssa-	O-INT-TRUS-060820/1663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server Platform Services (SPS) versions before SPS_E5_04.01.04.380.0, SPS_SoC-X_04.00.04.128.0, SPS_SoC-A_04.00.04.211.0, SPS_E3_04.01.04.109.0, SPS_E3_04.08.04.070.0 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2020-0545**	631949.pdf, https://kc.mcafee.com/corporate/index?page=content&id=SB10321	
Lenovo					
xiaoxin_air-15iwl_2019_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-XIAO-060820/1664
xiaoxin-14_2019iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-XIAO-060820/1665
xiaoxin-14iwl_qc_2019_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and	N/A	O-LEN-XIAO-060820/1666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
xiaoxin-15_2019iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-XIAO-060820/1667
y7000_2019_1050_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-Y700-060820/1668
yoga_730-13iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-YOGA-060820/1669
yoga_730-15iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function	N/A	O-LEN-YOGA-060820/1670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
yoga_s730-13iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-YOGA-060820/1671
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-YOGA-060820/1672
yoga_s940-14iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-YOGA-060820/1673
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo	N/A	O-LEN-YOGA-060820/1674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
flex_6-1470_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-FLEX-060820/1675
zhaoyang_k42-80_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-ZHAO-060820/1676
l340-15irh_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-L340-060820/1677
l340-17irh_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	O-LEN-L340-060820/1678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
l340-17iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-L340-060820/1679
legion_y530-15ich_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/1680
legion_y730-15ich_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/1681
legion_y7000p-1060_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/1682
legion_y730-17ich_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/1683
legion_y740-15irhg_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/1684
legion_y740-15ichg_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	O-LEN-LEGI-060820/1685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
legion_y9000k_2019_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/1686
legion_y740-17ichg_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/1687
legion_y740-17irhg_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/1688
legion_y9000p_2019_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may	N/A	O-LEN-LEGI-060820/1689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
lenovo_v720-14ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LENO-060820/1690
330-14ikbr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-330--060820/1691
330-15ikbr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-330--060820/1692
330-15ikbr_touch_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	O-LEN-330--060820/1693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
330-17ikbr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-330--060820/1694
720s_touch-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-720S-060820/1695
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-720S-060820/1696
720s-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo	N/A	O-LEN-720S-060820/1697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-720S-060820/1698
e53-80_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-E53--060820/1699
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-E53--060820/1700
k43c-80_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	O-LEN-K43C-060820/1701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
v330-14isk_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-V330-060820/1702
v330-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V330-060820/1703
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V330-060820/1704
v330-15isk_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V330-060820/1705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V330-060820/1706
v730-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V730-060820/1707
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V730-060820/1708
yoga_720-12ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-YOGA-060820/1709
yoga_730-13ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function	N/A	O-LEN-YOGA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		060820/1710
yoga_730-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-YOGA-060820/1711
yoga_c930-13ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-YOGA-060820/1712
thinkpad_11e_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1713
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad,	N/A	O-LEN-THIN-060820/1714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
miix_720-12ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-MIIX-060820/1715
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-MIIX-060820/1716
rescuer_y7000p_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-RESC-060820/1717
rescuer_y7000p\(1060\)_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may	N/A	O-LEN-RESC-060820/1718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
rescuer_y7000_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-RESC-060820/1719
rescuer_y7000\(1060\)_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-RESC-060820/1720
s145-14iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S145-060820/1721
s145-14ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	O-LEN-S145-060820/1722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
s145-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S145-060820/1723
s145-15iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S145-060820/1724
340c-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-340C-060820/1725
s340-14iwl_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S340-060820/1726
thinkstation_p410_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-THIN-060820/1727
thinkstation_p500_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-THIN-060820/1728
thinkstation_p510_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	O-LEN-THIN-060820/1729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
thinkstation_p520_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-THIN-060820/1730
thinkstation_p720_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-THIN-060820/1731
thinkstation_p910_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-THIN-060820/1732
thinkstation_p710_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may	N/A	O-LEN-THIN-060820/1733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
s340-14iwl_touch_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S340-060820/1734
s340-15iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S340-060820/1735
s340-15iwl_touch_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S340-060820/1736
s530-13iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	O-LEN-S530-060820/1737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
s540-14iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S540-060820/1738
s540-14iwl_touch_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S540-060820/1739
s540-15iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S540-060820/1740
s940-14iwl_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-S940-060820/1741
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-S940-060820/1742
v110-14ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V110-060820/1743
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V110-060820/1744
v130-14ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in	N/A	O-LEN-V130-060820/1745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
v130-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V130-060820/1746
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V130-060820/1747
v320-14ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-V320-060820/1748
v320-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and	N/A	O-LEN-V320-060820/1749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
v320-17ikbr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-V320-060820/1750
wei5-14ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-WEI5-060820/1751
wei5-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-WEI5-060820/1752
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo	N/A	O-LEN-WEI5-060820/1753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
xiaoxin_air_13iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-XIAO-060820/1754
xiaoxin_air_14ikbr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-XIAO-060820/1755
xiaoxin_air_14iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-XIAO-060820/1756
xiaoxin_air_15ikbr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	O-LEN-XIAO-060820/1757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
xiaoxin_air_15iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-XIAO-060820/1758
xiaoxin_air-14iwl_2019_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-XIAO-060820/1759
thinkpad_e490s_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1760
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo	N/A	O-LEN-THIN-060820/1761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/1762
thinkpad_s3_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1763
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1764
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/1765
thinkpad_11e_yoga_gen_6_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of	N/A	O-LEN-THIN-060820/1766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1767
thinkpad_yoga_11e_3rd_gen_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1768
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1769
thinkpad_yoga_11e_4th_gen_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1770
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo	N/A	O-LEN-THIN-060820/1771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_yoga_11e_5th_gen_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1772
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1773
thinkpad_13_2nd_gen_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1774
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1775
thinkpad_a285_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that	N/A	O-LEN-THIN-060820/1776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow escalation of privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1777
Incorrect Authorization	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	O-LEN-THIN-060820/1778
thinkpad_a485_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1779
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1780
Incorrect Authorization	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395,	N/A	O-LEN-THIN-060820/1781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**		
thinkpad_e14_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1782
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1783
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/1784
thinkpad_e15_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1785
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad,	N/A	O-LEN-THIN-060820/1786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/1787
thinkpad_r14_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1788
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1789
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/1790
thinkpad_s3_gen_2_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that	N/A	O-LEN-THIN-060820/1791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow escalation of privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1792
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/1793
thinkpad_e455_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1794
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1795
thinkpad_e555_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that	N/A	O-LEN-THIN-060820/1796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow escalation of privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1797
thinkpad_l13_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1798
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1799
legion_y7000p_2019_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/1800
legion_y7000p_pg0_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/1801
lenovo_e41-25_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LENO-060820/1802
lenovo_v320-17ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LENO-060820/1803
s145-14_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	O-LEN-S145-060820/1804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
s145-14igm_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S145-060820/1805
s145-15igm_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S145-060820/1806
s340-13iml_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S340-060820/1807
s340-14_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may	N/A	O-LEN-S340-060820/1808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
s340-14api_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S340-060820/1809
s340-14iil_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S340-060820/1810
s340-14iml_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S340-060820/1811
s340-15api_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	O-LEN-S340-060820/1812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
s340-15iml_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S340-060820/1813
s530-13iml_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S530-060820/1814
s540-14api_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S540-060820/1815
s540-14iml_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S540-060820/1816
s540-15iml_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S540-060820/1817
s540-15iwl_gtx_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-S540-060820/1818
s550-14iil_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	O-LEN-S550-060820/1819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
v130-14ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-V130-060820/1820
v130-14igm_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-V130-060820/1821
v130-15ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-V130-060820/1822
v145-14ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may	N/A	O-LEN-V145-060820/1823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
v145-15ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-V145-060820/1824
v330-14arr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-V330-060820/1825
v330-14ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-V330-060820/1826
v330-14igm_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	O-LEN-V330-060820/1827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
v330-15ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-V330-060820/1828
xiaoxin_air_14arr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-XIAO-060820/1829
xiaoxin-13iml_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-XIAO-060820/1830
xiaoxin-14igm_qc_2019_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-XIAO-060820/1831
xx-14kb_qc_2019_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-XX-1-060820/1832
yoga_530-14arr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-YOGA-060820/1833
yoga_c740-14iml_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	O-LEN-YOGA-060820/1834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
yoga_c740-15iml_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-YOGA-060820/1835
yoga_c930_glass_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-YOGA-060820/1836
yoga_c940_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-YOGA-060820/1837
yoga_s740-14iil_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may	N/A	O-LEN-YOGA-060820/1838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
yoga_530-14ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-YOGA-060820/1839
e43-80_kbl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-E43--060820/1840
thinkpad_s1_yoga_vpro_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1841
thinkpad_t540_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad,	N/A	O-LEN-THIN-060820/1842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_x1_carbon_\(20ax\)_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1843
thinkpad_x1_carbon_\(20bx\)_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1844
thinkpad_yoga_11e_\(20dx\)_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1845
thinkagile_2u4n_certified_node_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a	N/A	O-LEN-THIN-060820/1846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		
thinkagile_hx1320_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1847
thinkagile_hx1321_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1848
thinkagile_hx1520-r_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1849
thinkagile_hx1521-r_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of	N/A	O-LEN-THIN-060820/1850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		
thinkagile_hx2320_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1851
thinkagile_hx2320-e_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1852
thinkagile_hx2520-r_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkagile_hx2521-r_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1854
thinkagile_hx2710e_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1855
thinkagile_vx5520_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1856
thinkagile_vx7320-n_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to	N/A	O-LEN-THIN-060820/1857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system memory. **CVE ID : CVE-2020-8331**		
thinkagile_vx7520_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1858
thinkagile_vx7520-n_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1859
thinksystem_sr630_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1860
thinksystem_sr650_expansion_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA	N/A	O-LEN-THIN-060820/1861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		
thinksystem_sr650_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1862
vx_2u_certified_node_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-VX_2-060820/1863
thinksystem_dn8836_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1864
thinksystem_sd530_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		060820/1865
thinksystem_sd650_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1866
thinksystem_se350_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1867
thinksystem_sn550_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinksystem_sn850_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1869
thinksystem_sr150_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1870
thinksystem_sr250_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1871
thinksystem_sr258_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to	N/A	O-LEN-THIN-060820/1872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system memory. **CVE ID : CVE-2020-8331**		
thinksystem_sr530_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1873
thinksystem_sr550_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1874
thinksystem_sr570_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1875
thinksystem_sr590_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA	N/A	O-LEN-THIN-060820/1876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		
thinksystem_sr635_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1877
thinksystem_sr850_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1878
thinksystem_sr860_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1879
thinksystem_sr950_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		060820/1880
thinksystem_st250_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1881
thinksystem_st50_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1882
thinksystem_st550_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinksystem_st558_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/1884
thinkpad_l13_1st_gen_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/1885
thinkpad_l1415_gen_1_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/1886
thinkpad_p1_\(20mx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/1887
thinkpad_p1_\(20qx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB	N/A	O-LEN-THIN-060820/1888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**		
thinkpad_p52_\(20mx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/1889
thinkpad_p53_\(20qx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/1890
thinkpad_p53s_\(20nx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/1891
thinkstation_p520c_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code	N/A	O-LEN-THIN-060820/1892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-8321**		
thinkstation_p700_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-THIN-060820/1893
thinkstation_p900_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-THIN-060820/1894
thinkstation_p920_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-THIN-060820/1895
thinkpad_l1415_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of	N/A	O-LEN-THIN-060820/1896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1897
thinkpad_p43s_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1898
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1899
thinkpad_s5_2nd_gen_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1900
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo	N/A	O-LEN-THIN-060820/1901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_x395_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1902
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1903
Incorrect Authorization	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	O-LEN-THIN-060820/1904
thinkpad_s1_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1905
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad,	N/A	O-LEN-THIN-060820/1906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_t495_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1907
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1908
Incorrect Authorization	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	O-LEN-THIN-060820/1909
thinkpad_t495s_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1910
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	O-LEN-THIN-060820/1911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
Incorrect Authorizatio n	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	O-LEN-THIN-060820/1912
330-14ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-330--060820/1913
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-330--060820/1914
330-15ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	O-LEN-330--060820/1915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8322		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-330--060820/1916
330-17ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-330--060820/1917
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-330--060820/1918
340c-15api_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-340C-060820/1919
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	O-LEN-340C-060820/1920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
340c-15ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-340C-060820/1921
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-340C-060820/1922
c640-iml_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-C640-060820/1923
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	N/A	O-LEN-C640-060820/1924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8323		
k22-80_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-K22--060820/1925
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-K22--060820/1926
v720-12_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V720-060820/1927
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V720-060820/1928
k32-80_kbl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	O-LEN-K32--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		060820/1929
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-K32--060820/1930
k32-80_skl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-K32--060820/1931
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-K32--060820/1932
s145-14api_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation	N/A	O-LEN-S145-060820/1933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-S145-060820/1934
s145-14ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-S145-060820/1935
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-S145-060820/1936
s145-15api_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-S145-060820/1937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-S145-060820/1938
s145-15ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-S145-060820/1939
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-S145-060820/1940
s540-13api_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-S540-060820/1941
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad,	N/A	O-LEN-S540-060820/1942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
s750-iil_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-S750-060820/1943
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-S750-060820/1944
thinkbook_13s-iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-THIN-060820/1945
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	N/A	O-LEN-THIN-060820/1946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8323		
thinkbook_14s-iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-THIN-060820/1947
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1948
v110-14ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V110-060820/1949
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V110-060820/1950
v110-15ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	O-LEN-V110-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		060820/1951
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V110-060820/1952
v130-15igm_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V130-060820/1953
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V130-060820/1954
v310-15igm_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation	N/A	O-LEN-V310-060820/1955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V310-060820/1956
v340-iil_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V340-060820/1957
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V340-060820/1958
v340-iml_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V340-060820/1959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V340-060820/1960
v540s-13_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V540-060820/1961
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V540-060820/1962
14iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-14IW-060820/1963
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad,	N/A	O-LEN-14IW-060820/1964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
v730-13ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V730-060820/1965
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V730-060820/1966
v730-13isk_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V730-060820/1967
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	N/A	O-LEN-V730-060820/1968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8323		
xiaoxin_14-ast_qc_2019_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-XIAO-060820/1969
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-XIAO-060820/1970
xx-14api_qc_2019_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-XX-1-060820/1971
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-XX-1-060820/1972
6_pro-13-iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	O-LEN-6_PR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		060820/1973
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-6_PR-060820/1974
6_pro-14-iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-6_PR-060820/1975
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-6_PR-060820/1976
k3_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation	N/A	O-LEN-K3_F-060820/1977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-K3_F-060820/1978
k4-iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-K4-I-060820/1979
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-K4-I-060820/1980
130-14ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	O-LEN-130--060820/1981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
130-15ast_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-130--060820/1982
320c-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-320C-060820/1983
330-15arr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-330--060820/1984
330-15arr_touch_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may	N/A	O-LEN-330--060820/1985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
340c-15igm_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-340C-060820/1986
530s-14arr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-530S-060820/1987
720s-13arr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-720S-060820/1988
thinkpad_13_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that	N/A	O-LEN-THIN-060820/1989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow escalation of privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1990
thinkpad_a275_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1991
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1992
Incorrect Authorizatio n	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	O-LEN-THIN-060820/1993
thinkpad_a475_firmware					
Improper Privilege	09-06-2020	4.6	An internal shell was included in BIOS image in	N/A	O-LEN-THIN-060820/1994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1995
Incorrect Authorizatio n	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	O-LEN-THIN-060820/1996
thinkpad_e460_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/1997
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/1998
thinkpad_e560_firmware					
Improper	09-06-2020	4.6	An internal shell was	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**		060820/1999
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2000
thinkpad_e465_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2001
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2002
thinkpad_e565_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2003
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function	N/A	O-LEN-THIN-060820/2004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_e470_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2005
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2006
thinkpad_e570_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2007
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2008
thinkpad_e475_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2009
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2010
thinkpad_e575_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2011
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2012
thinkpad_e480_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2013
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		060820/2014
thinkpad_e580_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2015
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2016
thinkpad_e485_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2017
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_e585_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2019
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2020
thinkpad_s5_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2021
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2022
thinkpad_l380_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2024
thinkpad_l380_yoga_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2025
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2026
thinkpad_l460_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2027
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	N/A	O-LEN-THIN-060820/2028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8323		
thinkpad_l470_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2029
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2030
thinkpad_l480_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2031
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2032
thinkpad_l580_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege.	N/A	O-LEN-THIN-060820/2033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8320		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2034
thinkpad_l560_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2035
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2036
thinkpad_l570_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2037
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow	N/A	O-LEN-THIN-060820/2038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_p50_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2039
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2040
thinkpad_p50s_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2041
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2042
thinkpad_p51s_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of	N/A	O-LEN-THIN-060820/2043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2044
thinkagile_hx2720-e_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2045
thinkagile_hx3320_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2046
thinkagile_hx3321_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to	N/A	O-LEN-THIN-060820/2047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system memory. **CVE ID : CVE-2020-8331**		
thinkagile_hx3520-g_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2048
thinkagile_hx3521-g_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2049
thinkagile_hx3710_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2050
thinkagile_hx3720_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA	N/A	O-LEN-THIN-060820/2051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		
thinkagile_hx3721_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2052
thinkagile_hx3731_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2053
thinkagile_hx5520_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2054
thinkagile_hx5520-c_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		060820/2055
thinkagile_hx5521_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2056
thinkagile_hx5521-c_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2057
thinkagile_hx7520_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkagile_hx7521_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2059
thinkagile_hx7820_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2060
thinkagile_hx7821_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2061
thinkagile_mx_certified_node_all_flash_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to	N/A	O-LEN-THIN-060820/2062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system memory. **CVE ID : CVE-2020-8331**		
thinkagile_mx_certified_node_entry_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2063
thinkagile_mx_certified_node_hybrid_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2064
thinkagile_vx_1se_certified_node_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2065
thinkagile_vx_1u_certified_node_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA	N/A	O-LEN-THIN-060820/2066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		
thinkagile_vx_2u_certified_node_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2067
thinkagile_vx1320_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2068
thinkagile_vx2320_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2069
thinkagile_vx3320_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		060820/2070
thinkagile_vx3520-g_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2071
thinkagile_vx3720_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	O-LEN-THIN-060820/2072
130-14ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-130--060820/2073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
130-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-130--060820/2074
330-14ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-330--060820/2075
330-15ich_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-330--060820/2076
330-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code	N/A	O-LEN-330--060820/2077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-8321**		
330-17ich_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-330--060820/2078
330-17ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-330--060820/2079
330c-14ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-330C-060820/2080
330c-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in	N/A	O-LEN-330C-060820/2081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
330c-15ikbr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-330C-060820/2082
340c-15iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-340C-060820/2083
530s-14iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-530S-060820/2084
530s-15iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	O-LEN-530S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		060820/2085
530s-14ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-530S-060820/2086
530s-15ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-530S-060820/2087
720s-14ikbr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-720S-060820/2088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
730s-13iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-730S-060820/2089
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-730S-060820/2090
c340-14iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-C340-060820/2091
c340-15iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-C340-060820/2092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
e42-80_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-E42--060820/2093
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-E42--060820/2094
e52-80_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-E52--060820/2095
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-E52--060820/2096
flex_6-14ikb_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	O-LEN-FLEX-060820/2097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
flex-14iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-FLEX-060820/2098
flex-15iwl_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-FLEX-060820/2099
thinkpad_p52s_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2100
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo	N/A	O-LEN-THIN-060820/2101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_p70_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2102
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2103
thinkpad_e560p_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2104
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2105
thinkpad_t25_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that	N/A	O-LEN-THIN-060820/2106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow escalation of privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2107
thinkpad_t460_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2108
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2109
thinkpad_t460p_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2110
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad,	N/A	O-LEN-THIN-060820/2111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_t460s_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2112
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2113
thinkpad_t470_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2114
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2115
thinkpad_t470p_firmware					
Improper Privilege	09-06-2020	4.6	An internal shell was included in BIOS image in	N/A	O-LEN-THIN-060820/2116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2117
thinkpad_t470s_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2118
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2119
thinkpad_t480_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2120
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	O-LEN-THIN-060820/2121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_t480s_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2122
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2123
thinkpad_t560_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2124
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2125
thinkpad_t570_firmware					
Improper	09-06-2020	4.6	An internal shell was	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**		060820/2126
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2127
thinkpad_t580_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2128
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2129
thinkpad_x1_carbon_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2130
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function	N/A	O-LEN-THIN-060820/2131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_x1_yoga_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2132
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2133
thinkpad_x1_tablet_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2134
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2135
thinkpad_x260_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2136
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2137
thinkpad_x270_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2138
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2139
thinkpad_x280_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2140
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		060820/2141
thinkpad_x380_yoga_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2142
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2143
thinkpad_yoga_260_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2144
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_yoga_370_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2146
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2147
330-14igm_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-330--060820/2148
330-15igm_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-330--060820/2149
thinkpad_t440p_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		060820/2150
thinkpad_t490_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2151
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2152
thinkpad_t490s_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2153
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_t540p_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2155
thinkpad_t550_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2156
thinkpad_t590_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2157
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2158
thinkpad_w540_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	O-LEN-THIN-060820/2159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_w541_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2160
thinkpad_w550s_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2161
thinkpad_x1_extreme_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2162
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	N/A	O-LEN-THIN-060820/2163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8323		
thinkpad_x140e_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2164
thinkpad_x240_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2165
thinkpad_x240s_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2166
thinkpad_x250_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_x390_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2168
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2169
thinkpad_x390_yoga_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2170
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2171
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_s1_3rd_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2173
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2174
v330-15igm_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	O-LEN-V330-060820/2175
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-V330-060820/2176
thinkpad_p72_\(20mx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware	N/A	O-LEN-THIN-060820/2177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in flash. **CVE ID : CVE-2020-8336**		
thinkpad_p73_\(20qx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2178
thinkpad_t490_\(20nx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2179
thinkpad_t490_\(20qx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2180
thinkpad_t490_\(20rx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2181
thinkpad_t490s_\(20nx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**		060820/2182
thinkpad_t590_\(20nx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2183
thinkpad_x1_carbon_\(20qx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2184
thinkpad_x1_carbon_\(20rx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2185
thinkpad_x1_extreme_\(20mx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash.	N/A	O-LEN-THIN-060820/2186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8336		
thinkpad_x1_extreme_\(20qx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2187
thinkpad_x1_yoga_\(20qx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2188
thinkpad_x1_yoga_\(20sx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2189
thinkpad_x390_\(20qx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2190
thinkpad_x390_\(20sx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some	N/A	O-LEN-THIN-060820/2191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**		
thinkpad_e490_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2192
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2193
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2194
thinkpad_e590_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2195
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad,	N/A	O-LEN-THIN-060820/2196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2197
thinkpad_r490_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2198
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2199
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2200
thinkpad_r590_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that	N/A	O-LEN-THIN-060820/2201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow escalation of privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2202
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2203
thinkpad_helix_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2204
thinkpad_s3_3rd_gen_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2205
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	O-LEN-THIN-060820/2206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_s2_yoga_3rd_gen_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2207
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2208
thinkpad_l390_yoga_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2209
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2210
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB	N/A	O-LEN-THIN-060820/2211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**		
thinkpad_s2_yoga_4th_gen_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2212
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2213
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2214
thinkpad_l490_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2215
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	O-LEN-THIN-060820/2216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2217
thinkpad_l590_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2218
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2219
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2220
thinkpad_p1_firmware					
Improper Privilege	09-06-2020	4.6	An internal shell was included in BIOS image in	N/A	O-LEN-THIN-060820/2221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2222
thinkpad_p43s_\(20rx\)_firmware					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	O-LEN-THIN-060820/2223
thinkpad_p51_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2224
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2225
thinkpad_p52_firmware					
Improper	09-06-2020	4.6	An internal shell was	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**		060820/2226
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2227
thinkpad_p53_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2228
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2229
thinkpad_p53s_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2230
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function	N/A	O-LEN-THIN-060820/2231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_p71_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2232
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2233
thinkpad_p72_firmware					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2234
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2235
thinkpad_p73_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	O-LEN-THIN-060820/2236
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2237
thinkpad_s1_yoga_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2238
thinkpad_s5_yoga_15_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2239
thinkpad_s540_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo	N/A	O-LEN-THIN-060820/2240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_t440_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2241
thinkpad_t440s_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	O-LEN-THIN-060820/2242
c340-14api_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-C340-060820/2243
c340-14iml_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and	N/A	O-LEN-C340-060820/2244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
c340-15iil_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-C340-060820/2245
c340-15iml_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-C340-060820/2246
d330-10igm_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-D330-060820/2247
d335-10igm_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function	N/A	O-LEN-D335-060820/2248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
e4-14arr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-E4-1-060820/2249
flex_6-14arr_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-FLEX-060820/2250
ideapad_3_14_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-IDEA-060820/2251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ideapad_3_15_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-IDEA-060820/2252
ideapad_3_17iml05_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-IDEA-060820/2253
ideapad_3_15iil05_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-IDEA-060820/2254
ideapad_3_14iil05_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code	N/A	O-LEN-IDEA-060820/2255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-8321**		
ideapad_5_15iil05_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-IDEA-060820/2256
l3_15iml05_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-L3_1-060820/2257
l340-15api_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-L340-060820/2258
l340-15api_touch_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in	N/A	O-LEN-L340-060820/2259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
l340-15iwl_touch_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-L340-060820/2260
l340-17api_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-L340-060820/2261
legion_y530-15ich-1060_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/2262
legion_y540-15_pg0_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	O-LEN-LEGI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		060820/2263
legion_y540-15irh_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/2264
legion_y540-17_pg0_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/2265
legion_y540-17irh_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/2266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
legion_y545_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/2267
legion_y545_pg0_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/2268
legion_y7000_2019_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	O-LEN-LEGI-060820/2269
legion_y7000_pg0_firmware					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code	N/A	O-LEN-LEGI-060820/2270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-8321**		
Linux					
linux_kernel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-06-2020	4.3	IBM Security Guardium 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174739. **CVE ID : CVE-2020-4183**	https://www.ibm.com/support/pages/node/6220126	O-LIN-LINU-060820/2271
Use of a Broken or Risky Cryptographic Algorithm	04-06-2020	2.1	IBM Security Guardium 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174852. **CVE ID : CVE-2020-4191**	https://www.ibm.com/support/pages/node/6220130	O-LIN-LINU-060820/2272
Information Exposure	12-06-2020	3.6	A flaw was found in the Linux kernel's implementation of Userspace core dumps. This flaw allows an attacker with a local account to crash a trivial program and exfiltrate private kernel data. **CVE ID : CVE-2020-10732**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10732	O-LIN-LINU-060820/2273
Improper Privilege Management	09-06-2020	6.9	A flaw was found in the Linux Kernel in versions after 4.5-rc1 in the way mremap handled DAX Huge Pages. This flaw allows a	https://security.netapp.com/advisory/ntap-20200702-	O-LIN-LINU-060820/2274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local attacker with access to a DAX enabled storage to escalate their privileges on the system. **CVE ID : CVE-2020-10757**	0004/	
Use of Externally-Controlled Format String	09-06-2020	7.5	AnyDesk before 5.5.3 on Linux and FreeBSD has a format string vulnerability that can be exploited for remote code execution. **CVE ID : CVE-2020-13160**	N/A	O-LIN-LINU-060820/2275
Integer Overflow or Wraparound	09-06-2020	7.2	** DISPUTED ** An issue was discovered in the Linux kernel through 5.7.1. drivers/tty/vt/keyboard.c has an integer overflow if k_ascii is called several times in a row, aka CID-b86dab054059. NOTE: Members in the community argue that the integer overflow does not lead to a security issue in this case. **CVE ID : CVE-2020-13974**	N/A	O-LIN-LINU-060820/2276
Improper Restriction of Rendered UI Layers or Frames	15-06-2020	3.5	IBM Spectrum Protect Client 8.1.7.0 through 8.1.9.1 (Linux and Windows), 8.1.9.0 trough 8.1.9.1 (AIX) and IBM Spectrum Protect for Space Management 8.1.7.0 through 8.1.9.1 (Linux), 8.1.9.0 through 8.1.9.1 (AIX) web user interfaces could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could	https://www.ibm.com/support/pages/node/6221448	O-LIN-LINU-060820/2277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 179488. **CVE ID : CVE-2020-4406**		
Information Exposure	15-06-2020	5	IBM Spectrum Protect Client 8.1.7.0 through 8.1.9.1 (Linux and Windows), 8.1.9.0 trough 8.1.9.1 (AIX) and IBM Spectrum Protect for Space Management 8.1.7.0 through 8.1.9.1 (Linux), 8.1.9.0 through 8.1.9.1 (AIX) web user interfaces could allow an attacker to bypass authentication due to improper session validation which can result in access to unauthorized resources. IBM X-Force ID: 182019. **CVE ID : CVE-2020-4494**	https://www.ibm.com/support/pages/node/6221448	O-LIN-LINU-060820/2278
Improper Restriction of XML External Entity Reference ('XXE')	04-06-2020	5.5	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 182364. **CVE ID : CVE-2020-4509**	https://www.ibm.com/support/pages/node/6220154	O-LIN-LINU-060820/2279
Use After Free	12-06-2020	10	Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player	https://helpx.adobe.com/security	O-LIN-LINU-060820/2280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9633**	/products/flash-player/apsb20-30.html	
Microsoft					
windows					
Improper Restriction of Excessive Authentication Attempts	09-06-2020	3.3	Royal TS before 5 has a 0.0.0.0 listener, which makes it easier for attackers to bypass tunnel authentication via a brute-force approach. **CVE ID : CVE-2020-13872**	N/A	O-MIC-WIND-060820/2281
Improper Privilege Management	05-06-2020	7.2	An issue was discovered in Docker Desktop through 2.2.0.5 on Windows. If a local attacker sets up their own named pipe prior to starting Docker with the same name, this attacker can intercept a connection attempt from Docker Service (which runs as SYSTEM), and then impersonate their privileges. **CVE ID : CVE-2020-11492**	N/A	O-MIC-WIND-060820/2282
Improper Privilege Management	15-06-2020	4.6	VMware Horizon Client for Windows (prior to 5.4.3) contains a privilege escalation vulnerability due to folder permission configuration and unsafe loading of libraries. A local user on the system where the software is installed may	N/A	O-MIC-WIND-060820/2283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this issue to run commands as any user. **CVE ID : CVE-2020-3961**		
Improper Restriction of Rendered UI Layers or Frames	15-06-2020	3.5	IBM Spectrum Protect Client 8.1.7.0 through 8.1.9.1 (Linux and Windows), 8.1.9.0 trough 8.1.9.1 (AIX) and IBM Spectrum Protect for Space Management 8.1.7.0 through 8.1.9.1 (Linux), 8.1.9.0 through 8.1.9.1 (AIX) web user interfaces could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 179488. **CVE ID : CVE-2020-4406**	https://www.ibm.com/support/pages/node/6221448	O-MIC-WIND-060820/2284
Information Exposure	15-06-2020	5	IBM Spectrum Protect Client 8.1.7.0 through 8.1.9.1 (Linux and Windows), 8.1.9.0 trough 8.1.9.1 (AIX) and IBM Spectrum Protect for Space Management 8.1.7.0 through 8.1.9.1 (Linux), 8.1.9.0 through 8.1.9.1 (AIX) web user interfaces could allow an attacker to bypass authentication due to improper session validation which can result in access to unauthorized resources. IBM	https://www.ibm.com/support/pages/node/6221448	O-MIC-WIND-060820/2285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			X-Force ID: 182019. **CVE ID : CVE-2020-4494**		
Use After Free	12-06-2020	10	Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9633**	https://helpx.adobe.com/security/products/flash-player/apsb20-30.html	O-MIC-WIND-060820/2286
xbox_one					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	O-MIC-XBOX-060820/2287
windows_10					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-	N/A	O-MIC-WIND-060820/2288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0916. **CVE ID : CVE-2020-0915**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0915. **CVE ID : CVE-2020-0916**	N/A	O-MIC-WIND-060820/2289
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170. **CVE ID : CVE-2020-1163**	N/A	O-MIC-WIND-060820/2290
Improper Input Validation	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Shell does not properly validate file paths.An attacker who successfully exploited this vulnerability could run arbitrary code in the context of the current user, aka 'Windows Shell Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-060820/2291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1286		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1294. **CVE ID : CVE-2020-1287**	N/A	O-MIC-WIND-060820/2292
Improper Privilege Management	09-06-2020	9	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1317**	N/A	O-MIC-WIND-060820/2293
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-0986**	N/A	O-MIC-WIND-060820/2294
Improper Restriction of Operations	09-06-2020	9.3	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles	N/A	O-MIC-WIND-060820/2295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1073**		
Improper Input Validation	09-06-2020	4.9	A denial of service vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-1244. **CVE ID : CVE-2020-1120**	N/A	O-MIC-WIND-060820/2296
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1160**	N/A	O-MIC-WIND-060820/2297
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege (user to user) vulnerability exists in Windows Security Health Service when handling certain objects in memory.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1324. **CVE ID : CVE-2020-1162**	N/A	O-MIC-WIND-060820/2298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163. **CVE ID : CVE-2020-1170**	N/A	O-MIC-WIND-060820/2299
Improper Input Validation	09-06-2020	4.9	A denial of service vulnerability exists when Windows Registry improperly handles filesystem operations, aka 'Windows Registry Denial of Service Vulnerability'. **CVE ID : CVE-2020-1194**	N/A	O-MIC-WIND-060820/2300
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the printconfig.dll handles objects in memory, aka 'Windows Print Configuration Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1196**	N/A	O-MIC-WIND-060820/2301
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1197**	N/A	O-MIC-WIND-060820/2302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows Feedback Hub improperly handles objects in memory, aka 'Windows Feedback Hub Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1199**	N/A	O-MIC-WIND-060820/2303
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way the Windows Now Playing Session Manager handles objects in memory, aka 'Windows Now Playing Session Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1201**	N/A	O-MIC-WIND-060820/2304
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1203. **CVE ID : CVE-2020-1202**	N/A	O-MIC-WIND-060820/2305
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege	N/A	O-MIC-WIND-060820/2306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-1202. **CVE ID : CVE-2020-1203**		
Improper Privilege Management	09-06-2020	3.6	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1204**	N/A	O-MIC-WIND-060820/2307
Information Exposure	09-06-2020	5	An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1206**	N/A	O-MIC-WIND-060820/2308
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1247, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1207**	N/A	O-MIC-WIND-060820/2309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1236. **CVE ID : CVE-2020-1208**	N/A	O-MIC-WIND-060820/2310
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Network List Service handles objects in memory, aka 'Windows Network List Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1209**	N/A	O-MIC-WIND-060820/2311
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1211**	N/A	O-MIC-WIND-060820/2312
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when an OLE Automation component improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'OLE Automation Elevation of	N/A	O-MIC-WIND-060820/2313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. **CVE ID : CVE-2020-1212**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1213**	N/A	O-MIC-WIND-060820/2314
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1214**	N/A	O-MIC-WIND-060820/2315
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1215**	N/A	O-MIC-WIND-060820/2316
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory,	N/A	O-MIC-WIND-060820/2317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1216**		
Information Exposure	09-06-2020	6.8	An information disclosure vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1217**	N/A	O-MIC-WIND-060820/2318
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1219**	N/A	O-MIC-WIND-060820/2319
URL Redirection to Untrusted Site ('Open Redirect')	09-06-2020	5.8	A spoofing vulnerability exists when theMicrosoft Edge (Chromium-based) in IE Mode improperly handles specific redirects, aka 'Microsoft Edge (Chromium-based) in IE Mode Spoofing Vulnerability'. **CVE ID : CVE-2020-1220**	N/A	O-MIC-WIND-060820/2320
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Microsoft Store Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-060820/2321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution on the victim system, aka 'Microsoft Store Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1309. **CVE ID : CVE-2020-1222**		
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1260. **CVE ID : CVE-2020-1230**	N/A	O-MIC-WIND-060820/2322
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1231**	N/A	O-MIC-WIND-060820/2323
Out-of-bounds Read	09-06-2020	4.3	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1232**	N/A	O-MIC-WIND-060820/2324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1233**	N/A	O-MIC-WIND-060820/2325
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when Windows Error Reporting improperly handles objects in memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1234**	N/A	O-MIC-WIND-060820/2326
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1235**	N/A	O-MIC-WIND-060820/2327
Improper	09-06-2020	9.3	A remote code execution	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1208. **CVE ID : CVE-2020-1236**		060820/2328
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1237**	N/A	O-MIC-WIND-060820/2329
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1239. **CVE ID : CVE-2020-1238**	N/A	O-MIC-WIND-060820/2330
Improper Restriction of	09-06-2020	6.8	A memory corruption vulnerability exists when Windows Media Foundation	N/A	O-MIC-WIND-060820/2331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1238. **CVE ID : CVE-2020-1239**		
Improper Input Validation	09-06-2020	6.8	A security feature bypass vulnerability exists when Windows Kernel fails to properly sanitize certain parameters.To exploit the vulnerability, a locally-authenticated attacker could attempt to run a specially crafted application on a targeted system.The update addresses the vulnerability by correcting how Windows Kernel handles parameter sanitization., aka 'Windows Kernel Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1241**	N/A	O-MIC-WIND-060820/2332
Information Exposure	09-06-2020	2.6	An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests, aka 'Microsoft Edge Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1242**	N/A	O-MIC-WIND-060820/2333
N/A	09-06-2020	5.8	A denial of service vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and	N/A	O-MIC-WIND-060820/2334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Telemetry Service Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-1120. **CVE ID : CVE-2020-1244**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1246**	N/A	O-MIC-WIND-060820/2335
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1247**	N/A	O-MIC-WIND-060820/2336
Improper Restriction of Operations within the	09-06-2020	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the	N/A	O-MIC-WIND-060820/2337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1248**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1251**	N/A	O-MIC-WIND-060820/2338
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1310. **CVE ID : CVE-2020-1253**	N/A	O-MIC-WIND-060820/2339
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when Windows Modules Installer Service improperly handles class object members.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows	N/A	O-MIC-WIND-060820/2340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modules Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1254**		
Unrestricted Upload of File with Dangerous Type	09-06-2020	6.5	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1255**	N/A	O-MIC-WIND-060820/2341
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1278, CVE-2020-1293. **CVE ID : CVE-2020-1257**	N/A	O-MIC-WIND-060820/2342
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1258**	N/A	O-MIC-WIND-060820/2343
Insufficiently Protected Credentials	09-06-2020	4	A security feature bypass vulnerability exists when Windows Host Guardian Service improperly handles hashes recorded and logged,	N/A	O-MIC-WIND-060820/2344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'Windows Host Guardian Service Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1259**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230. **CVE ID : CVE-2020-1260**	N/A	O-MIC-WIND-060820/2345
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1263. **CVE ID : CVE-2020-1261**	N/A	O-MIC-WIND-060820/2346
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275,	N/A	O-MIC-WIND-060820/2347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1262**		
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1261. **CVE ID : CVE-2020-1263**	N/A	O-MIC-WIND-060820/2348
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1264**	N/A	O-MIC-WIND-060820/2349
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233,	N/A	O-MIC-WIND-060820/2350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1235, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1265**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1266**	N/A	O-MIC-WIND-060820/2351
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when a Windows service improperly handles objects in memory, aka 'Windows Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1268**	N/A	O-MIC-WIND-060820/2352
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-	N/A	O-MIC-WIND-060820/2353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1266, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1269**		
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	O-MIC-WIND-060820/2354
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the wlansvc.dll handles objects in memory, aka 'Windows WLAN Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1270**	N/A	O-MIC-WIND-060820/2355
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1271**	N/A	O-MIC-WIND-060820/2356
Improper Privilege	09-06-2020	7.2	An elevation of privilege vulnerability exists in the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1277, CVE-2020-1302, CVE-2020-1312. **CVE ID : CVE-2020-1272**		060820/2357
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1273**	N/A	O-MIC-WIND-060820/2358
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-	N/A	O-MIC-WIND-060820/2359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1274**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1275**	N/A	O-MIC-WIND-060820/2360
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1276**	N/A	O-MIC-WIND-060820/2361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1302, CVE-2020-1312. **CVE ID : CVE-2020-1277**	N/A	O-MIC-WIND-060820/2362
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1293. **CVE ID : CVE-2020-1278**	N/A	O-MIC-WIND-060820/2363
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when Windows Lockscreen fails to properly load spotlight images from a secure location, aka 'Windows Lockscreen Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1279**	N/A	O-MIC-WIND-060820/2364
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows	N/A	O-MIC-WIND-060820/2365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bluetooth Service handles objects in memory, aka 'Windows Bluetooth Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1280**		
Improper Input Validation	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1281**	N/A	O-MIC-WIND-060820/2366
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1282**	N/A	O-MIC-WIND-060820/2367
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.1	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2020-1283**	N/A	O-MIC-WIND-060820/2368
N/A	09-06-2020	4.3	A denial of service vulnerability exists in the way that the Microsoft Server Message Block 3.1.1	N/A	O-MIC-WIND-060820/2369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Denial of Service Vulnerability'. **CVE ID : CVE-2020-1284**		
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1290**	N/A	O-MIC-WIND-060820/2370
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1291**	N/A	O-MIC-WIND-060820/2371
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in OpenSSH for Windows when it does not properly restrict access to configuration settings, aka 'OpenSSH for Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1292**	N/A	O-MIC-WIND-060820/2372
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard	N/A	O-MIC-WIND-060820/2373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1278. **CVE ID : CVE-2020-1293**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1287. **CVE ID : CVE-2020-1294**	N/A	O-MIC-WIND-060820/2374
Information Exposure	09-06-2020	2.1	A vulnerability exists in the way the Windows Diagnostics & feedback settings app handles objects in memory, aka 'Windows Diagnostics & feedback Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1296**	N/A	O-MIC-WIND-060820/2375
N/A	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1299**	N/A	O-MIC-WIND-060820/2376
N/A	09-06-2020	6.8	A remote code execution vulnerability exists when	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Windows fails to properly handle cabinet files.To exploit the vulnerability, an attacker would have to convince a user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.The update addresses the vulnerability by correcting how Windows handles cabinet files., aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1300**		060820/2377
N/A	09-06-2020	6.5	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1301**	N/A	O-MIC-WIND-060820/2378
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-060820/2379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1272, CVE-2020-1277, CVE-2020-1312. **CVE ID : CVE-2020-1302**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1304**	N/A	O-MIC-WIND-060820/2380
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1305**	N/A	O-MIC-WIND-060820/2381
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1334. **CVE ID : CVE-2020-1306**	N/A	O-MIC-WIND-060820/2382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	9.3	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1316. **CVE ID : CVE-2020-1307**	N/A	O-MIC-WIND-060820/2383
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Microsoft Store Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Microsoft Store Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1222. **CVE ID : CVE-2020-1309**	N/A	O-MIC-WIND-060820/2384
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247,	N/A	O-MIC-WIND-060820/2385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1251, CVE-2020-1253. **CVE ID : CVE-2020-1310**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when Component Object Model (COM) client uses special case IIDs, aka 'Component Object Model Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1311**	N/A	O-MIC-WIND-060820/2386
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1277, CVE-2020-1302. **CVE ID : CVE-2020-1312**	N/A	O-MIC-WIND-060820/2387
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Update Orchestrator Service improperly handles file operations, aka 'Windows Update Orchestrator Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1313**	N/A	O-MIC-WIND-060820/2388
Improper Privilege	09-06-2020	6.8	An elevation of privilege vulnerability exists in	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Text Service Framework (TSF) when the TSF server fails to properly handle messages sent from TSF clients, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1314**		060820/2389
Information Exposure	09-06-2020	2.6	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory, aka 'Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1315**	N/A	O-MIC-WIND-060820/2390
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307. **CVE ID : CVE-2020-1316**	N/A	O-MIC-WIND-060820/2391
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege (user to user) vulnerability exists in Windows Security Health Service when handling certain objects in memory.To exploit the	N/A	O-MIC-WIND-060820/2392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would first have to log on to the system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1162. **CVE ID : CVE-2020-1324**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306. **CVE ID : CVE-2020-1334**	N/A	O-MIC-WIND-060820/2393
Information Exposure	09-06-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1348**	N/A	O-MIC-WIND-060820/2394
Use After Free	12-06-2020	10	Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free vulnerability. Successful	https://helpx.adobe.com/security/products/flash-player/apsb20-30.html	O-MIC-WIND-060820/2395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9633**		
windows_7					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170. **CVE ID : CVE-2020-1163**	N/A	O-MIC-WIND-060820/2396
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1294. **CVE ID : CVE-2020-1287**	N/A	O-MIC-WIND-060820/2397
Improper Privilege Management	09-06-2020	9	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1317**	N/A	O-MIC-WIND-060820/2398
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when the	N/A	O-MIC-WIND-060820/2399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1160**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163. **CVE ID : CVE-2020-1170**	N/A	O-MIC-WIND-060820/2400
Improper Input Validation	09-06-2020	4.9	A denial of service vulnerability exists when Windows Registry improperly handles filesystem operations, aka 'Windows Registry Denial of Service Vulnerability'. **CVE ID : CVE-2020-1194**	N/A	O-MIC-WIND-060820/2401
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the printconfig.dll handles objects in memory, aka 'Windows Print Configuration Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1196**	N/A	O-MIC-WIND-060820/2402
Improper Privilege	09-06-2020	7.2	An elevation of privilege vulnerability exists in	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1247, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1207**		060820/2403
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1236. **CVE ID : CVE-2020-1208**	N/A	O-MIC-WIND-060820/2404
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when an OLE Automation component improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'OLE Automation Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1212**	N/A	O-MIC-WIND-060820/2405
Improper Restriction of Operations within the	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code	N/A	O-MIC-WIND-060820/2406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Execution Vulnerability'. This CVE ID is unique from CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1213**		
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1214**	N/A	O-MIC-WIND-060820/2407
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1215**	N/A	O-MIC-WIND-060820/2408
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1216**	N/A	O-MIC-WIND-060820/2409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1219**	N/A	O-MIC-WIND-060820/2410
URL Redirection to Untrusted Site ('Open Redirect')	09-06-2020	5.8	A spoofing vulnerability exists when theMicrosoft Edge (Chromium-based) in IE Mode improperly handles specific redirects, aka 'Microsoft Edge (Chromium-based) in IE Mode Spoofing Vulnerability'. **CVE ID : CVE-2020-1220**	N/A	O-MIC-WIND-060820/2411
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1260. **CVE ID : CVE-2020-1230**	N/A	O-MIC-WIND-060820/2412
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1208. **CVE ID : CVE-2020-1236**	N/A	O-MIC-WIND-060820/2413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1238. **CVE ID : CVE-2020-1239**	N/A	O-MIC-WIND-060820/2414
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1246**	N/A	O-MIC-WIND-060820/2415
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1247**	N/A	O-MIC-WIND-060820/2416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1251**	N/A	O-MIC-WIND-060820/2417
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1310. **CVE ID : CVE-2020-1253**	N/A	O-MIC-WIND-060820/2418
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when Windows Modules Installer Service improperly handles class object members.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Modules Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1254**	N/A	O-MIC-WIND-060820/2419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	09-06-2020	6.5	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1255**	N/A	O-MIC-WIND-060820/2420
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230. **CVE ID : CVE-2020-1260**	N/A	O-MIC-WIND-060820/2421
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1262**	N/A	O-MIC-WIND-060820/2422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1261. **CVE ID : CVE-2020-1263**	N/A	O-MIC-WIND-060820/2423
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1269**	N/A	O-MIC-WIND-060820/2424
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the wlansvc.dll handles objects in memory, aka 'Windows WLAN Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1270**	N/A	O-MIC-WIND-060820/2425
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file	N/A	O-MIC-WIND-060820/2426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1271**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1277, CVE-2020-1302, CVE-2020-1312. **CVE ID : CVE-2020-1272**	N/A	O-MIC-WIND-060820/2427
Improper Input Validation	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1281**	N/A	O-MIC-WIND-060820/2428
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-060820/2429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1291**		
N/A	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1299**	N/A	O-MIC-WIND-060820/2430
N/A	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows fails to properly handle cabinet files.To exploit the vulnerability, an attacker would have to convince a user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.The update addresses the vulnerability by correcting how Windows handles cabinet files., aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1300**	N/A	O-MIC-WIND-060820/2431
N/A	09-06-2020	6.5	A remote code execution vulnerability exists in the way that the Microsoft	N/A	O-MIC-WIND-060820/2432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server Message Block 1.0 (SMBv1) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1301**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1277, CVE-2020-1312. **CVE ID : CVE-2020-1302**	N/A	O-MIC-WIND-060820/2433
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when Component Object Model (COM) client uses special case IIDs, aka 'Component Object Model Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1311**	N/A	O-MIC-WIND-060820/2434
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server fails to properly handle messages sent from TSF clients, aka 'Windows Text Service Framework Elevation of Privilege	N/A	O-MIC-WIND-060820/2435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1314**		
Information Exposure	09-06-2020	2.6	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory, aka 'Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1315**	N/A	O-MIC-WIND-060820/2436
Information Exposure	09-06-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1348**	N/A	O-MIC-WIND-060820/2437
windows_8.1					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0916. **CVE ID : CVE-2020-0915**	N/A	O-MIC-WIND-060820/2438
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-060820/2439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2020-0915. **CVE ID : CVE-2020-0916**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170. **CVE ID : CVE-2020-1163**	N/A	O-MIC-WIND-060820/2440
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1294. **CVE ID : CVE-2020-1287**	N/A	O-MIC-WIND-060820/2441
Improper Privilege Management	09-06-2020	9	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1317**	N/A	O-MIC-WIND-060820/2442
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in	N/A	O-MIC-WIND-060820/2443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-0986**		
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1160**	N/A	O-MIC-WIND-060820/2444
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163. **CVE ID : CVE-2020-1170**	N/A	O-MIC-WIND-060820/2445
Improper Input Validation	09-06-2020	4.9	A denial of service vulnerability exists when Windows Registry improperly handles	N/A	O-MIC-WIND-060820/2446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			filesystem operations, aka 'Windows Registry Denial of Service Vulnerability'. **CVE ID : CVE-2020-1194**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the printconfig.dll handles objects in memory, aka 'Windows Print Configuration Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1196**	N/A	O-MIC-WIND-060820/2447
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1247, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1207**	N/A	O-MIC-WIND-060820/2448
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1236. **CVE ID : CVE-2020-1208**	N/A	O-MIC-WIND-060820/2449
Improper Privilege	09-06-2020	6.8	An elevation of privilege vulnerability exists when an OLE Automation component	N/A	O-MIC-WIND-060820/2450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'OLE Automation Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1212**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1213**	N/A	O-MIC-WIND-060820/2451
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1214**	N/A	O-MIC-WIND-060820/2452
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-	N/A	O-MIC-WIND-060820/2453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1214, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1215**		
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1216**	N/A	O-MIC-WIND-060820/2454
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1219**	N/A	O-MIC-WIND-060820/2455
URL Redirection to Untrusted Site ('Open Redirect')	09-06-2020	5.8	A spoofing vulnerability exists when theMicrosoft Edge (Chromium-based) in IE Mode improperly handles specific redirects, aka 'Microsoft Edge (Chromium-based) in IE Mode Spoofing Vulnerability'. **CVE ID : CVE-2020-1220**	N/A	O-MIC-WIND-060820/2456
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-	N/A	O-MIC-WIND-060820/2457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1260. **CVE ID : CVE-2020-1230**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1231**	N/A	O-MIC-WIND-060820/2458
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1208. **CVE ID : CVE-2020-1236**	N/A	O-MIC-WIND-060820/2459
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1238. **CVE ID : CVE-2020-1239**	N/A	O-MIC-WIND-060820/2460
Improper Privilege	09-06-2020	7.2	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1246**		060820/2461
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1247**	N/A	O-MIC-WIND-060820/2462
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1253, CVE-2020-1310.	N/A	O-MIC-WIND-060820/2463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1251		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1310. **CVE ID : CVE-2020-1253**	N/A	O-MIC-WIND-060820/2464
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when Windows Modules Installer Service improperly handles class object members.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Modules Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1254**	N/A	O-MIC-WIND-060820/2465
Unrestricted Upload of File with Dangerous Type	09-06-2020	6.5	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1255**	N/A	O-MIC-WIND-060820/2466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230. **CVE ID : CVE-2020-1260**	N/A	O-MIC-WIND-060820/2467
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1262**	N/A	O-MIC-WIND-060820/2468
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1261. **CVE ID : CVE-2020-1263**	N/A	O-MIC-WIND-060820/2469
Improper	09-06-2020	7.2	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1269**		060820/2470
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the wlansvc.dll handles objects in memory, aka 'Windows WLAN Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1270**	N/A	O-MIC-WIND-060820/2471
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1277, CVE-2020-1302, CVE-2020-1312.	N/A	O-MIC-WIND-060820/2472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1272		
Improper Input Validation	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1281**	N/A	O-MIC-WIND-060820/2473
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1282**	N/A	O-MIC-WIND-060820/2474
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1291**	N/A	O-MIC-WIND-060820/2475
N/A	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this	N/A	O-MIC-WIND-060820/2476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1299**		
N/A	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows fails to properly handle cabinet files.To exploit the vulnerability, an attacker would have to convince a user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.The update addresses the vulnerability by correcting how Windows handles cabinet files., aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1300**	N/A	O-MIC-WIND-060820/2477
N/A	09-06-2020	6.5	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1301**	N/A	O-MIC-WIND-060820/2478
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain	N/A	O-MIC-WIND-060820/2479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1277, CVE-2020-1312. **CVE ID : CVE-2020-1302**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1253. **CVE ID : CVE-2020-1310**	N/A	O-MIC-WIND-060820/2480
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when Component Object Model (COM) client uses special case IIDs, aka 'Component Object Model Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1311**	N/A	O-MIC-WIND-060820/2481
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server fails to properly handle messages sent from TSF clients, aka 'Windows	N/A	O-MIC-WIND-060820/2482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1314**		
Information Exposure	09-06-2020	2.6	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory, aka 'Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1315**	N/A	O-MIC-WIND-060820/2483
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306. **CVE ID : CVE-2020-1334**	N/A	O-MIC-WIND-060820/2484
Information Exposure	09-06-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1348**	N/A	O-MIC-WIND-060820/2485
Use After Free	12-06-2020	10	Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for	https://helpx.adobe.com/security/products/flash-player/apsb	O-MIC-WIND-060820/2486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9633**	20-30.html	
windows_rt_8.1					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0916. **CVE ID : CVE-2020-0915**	N/A	O-MIC-WIND-060820/2487
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0915. **CVE ID : CVE-2020-0916**	N/A	O-MIC-WIND-060820/2488
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender	N/A	O-MIC-WIND-060820/2489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170. **CVE ID : CVE-2020-1163**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1294. **CVE ID : CVE-2020-1287**	N/A	O-MIC-WIND-060820/2490
Improper Privilege Management	09-06-2020	9	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1317**	N/A	O-MIC-WIND-060820/2491
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-0986**	N/A	O-MIC-WIND-060820/2492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1160**	N/A	O-MIC-WIND-060820/2493
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163. **CVE ID : CVE-2020-1170**	N/A	O-MIC-WIND-060820/2494
Improper Input Validation	09-06-2020	4.9	A denial of service vulnerability exists when Windows Registry improperly handles filesystem operations, aka 'Windows Registry Denial of Service Vulnerability'. **CVE ID : CVE-2020-1194**	N/A	O-MIC-WIND-060820/2495
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the printconfig.dll handles objects in memory, aka 'Windows Print Configuration Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1196**	N/A	O-MIC-WIND-060820/2496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1247, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1207**	N/A	O-MIC-WIND-060820/2497
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1236. **CVE ID : CVE-2020-1208**	N/A	O-MIC-WIND-060820/2498
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when an OLE Automation component improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'OLE Automation Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1212**	N/A	O-MIC-WIND-060820/2499
Improper Restriction of	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine	N/A	O-MIC-WIND-060820/2500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1213**		
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1214**	N/A	O-MIC-WIND-060820/2501
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1215**	N/A	O-MIC-WIND-060820/2502
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-	N/A	O-MIC-WIND-060820/2503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1216**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1219**	N/A	O-MIC-WIND-060820/2504
URL Redirection to Untrusted Site ('Open Redirect')	09-06-2020	5.8	A spoofing vulnerability exists when theMicrosoft Edge (Chromium-based) in IE Mode improperly handles specific redirects, aka 'Microsoft Edge (Chromium-based) in IE Mode Spoofing Vulnerability'. **CVE ID : CVE-2020-1220**	N/A	O-MIC-WIND-060820/2505
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1260. **CVE ID : CVE-2020-1230**	N/A	O-MIC-WIND-060820/2506
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1233, CVE-2020-1235,	N/A	O-MIC-WIND-060820/2507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1231**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1208. **CVE ID : CVE-2020-1236**	N/A	O-MIC-WIND-060820/2508
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1238. **CVE ID : CVE-2020-1239**	N/A	O-MIC-WIND-060820/2509
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-	N/A	O-MIC-WIND-060820/2510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1307, CVE-2020-1316. **CVE ID : CVE-2020-1246**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1247**	N/A	O-MIC-WIND-060820/2511
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1251**	N/A	O-MIC-WIND-060820/2512
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-	N/A	O-MIC-WIND-060820/2513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1310. **CVE ID : CVE-2020-1253**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when Windows Modules Installer Service improperly handles class object members.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Modules Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1254**	N/A	O-MIC-WIND-060820/2514
Unrestricted Upload of File with Dangerous Type	09-06-2020	6.5	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1255**	N/A	O-MIC-WIND-060820/2515
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230. **CVE ID : CVE-2020-1260**	N/A	O-MIC-WIND-060820/2516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1262**	N/A	O-MIC-WIND-060820/2517
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1261. **CVE ID : CVE-2020-1263**	N/A	O-MIC-WIND-060820/2518
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275,	N/A	O-MIC-WIND-060820/2519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1269**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the wlansvc.dll handles objects in memory, aka 'Windows WLAN Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1270**	N/A	O-MIC-WIND-060820/2520
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1277, CVE-2020-1302, CVE-2020-1312. **CVE ID : CVE-2020-1272**	N/A	O-MIC-WIND-060820/2521
Improper Input Validation	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1281**	N/A	O-MIC-WIND-060820/2522
Improper Privilege	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime	N/A	O-MIC-WIND-060820/2523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1282**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1291**	N/A	O-MIC-WIND-060820/2524
N/A	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1299**	N/A	O-MIC-WIND-060820/2525
N/A	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows fails to properly handle cabinet files.To exploit the vulnerability, an attacker would have to convince a	N/A	O-MIC-WIND-060820/2526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.The update addresses the vulnerability by correcting how Windows handles cabinet files., aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1300**		
N/A	09-06-2020	6.5	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1301**	N/A	O-MIC-WIND-060820/2527
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1277, CVE-2020-1312. **CVE ID : CVE-2020-1302**	N/A	O-MIC-WIND-060820/2528
Improper	09-06-2020	7.2	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1253. **CVE ID : CVE-2020-1310**		060820/2529
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when Component Object Model (COM) client uses special case IIDs, aka 'Component Object Model Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1311**	N/A	O-MIC-WIND-060820/2530
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server fails to properly handle messages sent from TSF clients, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1314**	N/A	O-MIC-WIND-060820/2531
Information Exposure	09-06-2020	2.6	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory, aka 'Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1315**	N/A	O-MIC-WIND-060820/2532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306. **CVE ID : CVE-2020-1334**	N/A	O-MIC-WIND-060820/2533
Information Exposure	09-06-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1348**	N/A	O-MIC-WIND-060820/2534
windows_server_2008					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170. **CVE ID : CVE-2020-1163**	N/A	O-MIC-WIND-060820/2535
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows	N/A	O-MIC-WIND-060820/2536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1294. **CVE ID : CVE-2020-1287**		
Improper Privilege Management	09-06-2020	9	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1317**	N/A	O-MIC-WIND-060820/2537
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1160**	N/A	O-MIC-WIND-060820/2538
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163. **CVE ID : CVE-2020-1170**	N/A	O-MIC-WIND-060820/2539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-06-2020	4.9	A denial of service vulnerability exists when Windows Registry improperly handles filesystem operations, aka 'Windows Registry Denial of Service Vulnerability'. **CVE ID : CVE-2020-1194**	N/A	O-MIC-WIND-060820/2540
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the printconfig.dll handles objects in memory, aka 'Windows Print Configuration Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1196**	N/A	O-MIC-WIND-060820/2541
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1247, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1207**	N/A	O-MIC-WIND-060820/2542
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1236.	N/A	O-MIC-WIND-060820/2543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1208		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when an OLE Automation component improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'OLE Automation Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1212**	N/A	O-MIC-WIND-060820/2544
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1213**	N/A	O-MIC-WIND-060820/2545
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1214**	N/A	O-MIC-WIND-060820/2546
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory,	N/A	O-MIC-WIND-060820/2547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1215**		
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1216**	N/A	O-MIC-WIND-060820/2548
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1219**	N/A	O-MIC-WIND-060820/2549
URL Redirection to Untrusted Site ('Open Redirect')	09-06-2020	5.8	A spoofing vulnerability exists when theMicrosoft Edge (Chromium-based) in IE Mode improperly handles specific redirects, aka 'Microsoft Edge (Chromium-based) in IE Mode Spoofing Vulnerability'. **CVE ID : CVE-2020-1220**	N/A	O-MIC-WIND-060820/2550
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory,	N/A	O-MIC-WIND-060820/2551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1260. **CVE ID : CVE-2020-1230**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1208. **CVE ID : CVE-2020-1236**	N/A	O-MIC-WIND-060820/2552
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1238. **CVE ID : CVE-2020-1239**	N/A	O-MIC-WIND-060820/2553
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-	N/A	O-MIC-WIND-060820/2554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1246**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1247**	N/A	O-MIC-WIND-060820/2555
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1251**	N/A	O-MIC-WIND-060820/2556
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-060820/2557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1310. **CVE ID : CVE-2020-1253**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when Windows Modules Installer Service improperly handles class object members.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Modules Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1254**	N/A	O-MIC-WIND-060820/2558
Unrestricted Upload of File with Dangerous Type	09-06-2020	6.5	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1255**	N/A	O-MIC-WIND-060820/2559
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-	N/A	O-MIC-WIND-060820/2560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1216, CVE-2020-1230. **CVE ID : CVE-2020-1260**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1262**	N/A	O-MIC-WIND-060820/2561
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1261. **CVE ID : CVE-2020-1263**	N/A	O-MIC-WIND-060820/2562
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262,	N/A	O-MIC-WIND-060820/2563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1264, CVE-2020-1266, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1269**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the wlansvc.dll handles objects in memory, aka 'Windows WLAN Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1270**	N/A	O-MIC-WIND-060820/2564
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1271**	N/A	O-MIC-WIND-060820/2565
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-060820/2566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2020-1277, CVE-2020-1302, CVE-2020-1312. **CVE ID : CVE-2020-1272**		
Improper Input Validation	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1281**	N/A	O-MIC-WIND-060820/2567
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1291**	N/A	O-MIC-WIND-060820/2568
N/A	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1299**	N/A	O-MIC-WIND-060820/2569
N/A	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows fails to properly handle cabinet files.To exploit the	N/A	O-MIC-WIND-060820/2570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would have to convince a user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.The update addresses the vulnerability by correcting how Windows handles cabinet files., aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1300**		
N/A	09-06-2020	6.5	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1301**	N/A	O-MIC-WIND-060820/2571
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1277, CVE-2020-1312.	N/A	O-MIC-WIND-060820/2572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1302		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when Component Object Model (COM) client uses special case IIDs, aka 'Component Object Model Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1311**	N/A	O-MIC-WIND-060820/2573
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server fails to properly handle messages sent from TSF clients, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1314**	N/A	O-MIC-WIND-060820/2574
Information Exposure	09-06-2020	2.6	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory, aka 'Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1315**	N/A	O-MIC-WIND-060820/2575
Information Exposure	09-06-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1348**	N/A	O-MIC-WIND-060820/2576
windows_server_2012					
Improper	09-06-2020	7.2	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0916. **CVE ID : CVE-2020-0915**		060820/2577
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0915. **CVE ID : CVE-2020-0916**	N/A	O-MIC-WIND-060820/2578
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170. **CVE ID : CVE-2020-1163**	N/A	O-MIC-WIND-060820/2579
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles	N/A	O-MIC-WIND-060820/2580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1294. **CVE ID : CVE-2020-1287**		
Improper Privilege Management	09-06-2020	9	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1317**	N/A	O-MIC-WIND-060820/2581
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-0986**	N/A	O-MIC-WIND-060820/2582
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1160**	N/A	O-MIC-WIND-060820/2583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163. **CVE ID : CVE-2020-1170**	N/A	O-MIC-WIND-060820/2584
Improper Input Validation	09-06-2020	4.9	A denial of service vulnerability exists when Windows Registry improperly handles filesystem operations, aka 'Windows Registry Denial of Service Vulnerability'. **CVE ID : CVE-2020-1194**	N/A	O-MIC-WIND-060820/2585
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the printconfig.dll handles objects in memory, aka 'Windows Print Configuration Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1196**	N/A	O-MIC-WIND-060820/2586
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-060820/2587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1247, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1207**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1236. **CVE ID : CVE-2020-1208**	N/A	O-MIC-WIND-060820/2588
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when an OLE Automation component improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'OLE Automation Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1212**	N/A	O-MIC-WIND-060820/2589
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1213**	N/A	O-MIC-WIND-060820/2590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1214**	N/A	O-MIC-WIND-060820/2591
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1215**	N/A	O-MIC-WIND-060820/2592
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1216**	N/A	O-MIC-WIND-060820/2593
Improper Restriction of Operations within the Bounds of a	09-06-2020	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption	N/A	O-MIC-WIND-060820/2594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Vulnerability'. **CVE ID : CVE-2020-1219**		
URL Redirection to Untrusted Site ('Open Redirect')	09-06-2020	5.8	A spoofing vulnerability exists when theMicrosoft Edge (Chromium-based) in IE Mode improperly handles specific redirects, aka 'Microsoft Edge (Chromium-based) in IE Mode Spoofing Vulnerability'. **CVE ID : CVE-2020-1220**	N/A	O-MIC-WIND-060820/2595
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1260. **CVE ID : CVE-2020-1230**	N/A	O-MIC-WIND-060820/2596
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1231**	N/A	O-MIC-WIND-060820/2597
Improper Restriction of Operations	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles	N/A	O-MIC-WIND-060820/2598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1208. **CVE ID : CVE-2020-1236**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1238. **CVE ID : CVE-2020-1239**	N/A	O-MIC-WIND-060820/2599
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1246**	N/A	O-MIC-WIND-060820/2600
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory,	N/A	O-MIC-WIND-060820/2601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1247**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1251**	N/A	O-MIC-WIND-060820/2602
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1310. **CVE ID : CVE-2020-1253**	N/A	O-MIC-WIND-060820/2603
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when Windows Modules Installer Service improperly handles class object members.A locally authenticated	N/A	O-MIC-WIND-060820/2604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could run arbitrary code with elevated system privileges, aka 'Windows Modules Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1254**		
Unrestricted Upload of File with Dangerous Type	09-06-2020	6.5	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1255**	N/A	O-MIC-WIND-060820/2605
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230. **CVE ID : CVE-2020-1260**	N/A	O-MIC-WIND-060820/2606
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-	N/A	O-MIC-WIND-060820/2607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1246, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1262**		
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1261. **CVE ID : CVE-2020-1263**	N/A	O-MIC-WIND-060820/2608
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1269**	N/A	O-MIC-WIND-060820/2609
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the wlansvc.dll handles objects in memory, aka 'Windows WLAN Service	N/A	O-MIC-WIND-060820/2610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1270**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1277, CVE-2020-1302, CVE-2020-1312. **CVE ID : CVE-2020-1272**	N/A	O-MIC-WIND-060820/2611
Improper Input Validation	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1281**	N/A	O-MIC-WIND-060820/2612
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1304, CVE-	N/A	O-MIC-WIND-060820/2613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1282**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1291**	N/A	O-MIC-WIND-060820/2614
N/A	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1299**	N/A	O-MIC-WIND-060820/2615
N/A	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows fails to properly handle cabinet files.To exploit the vulnerability, an attacker would have to convince a user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.The update addresses the vulnerability by	N/A	O-MIC-WIND-060820/2616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			correcting how Windows handles cabinet files., aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1300**		
N/A	09-06-2020	6.5	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1301**	N/A	O-MIC-WIND-060820/2617
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1277, CVE-2020-1312. **CVE ID : CVE-2020-1302**	N/A	O-MIC-WIND-060820/2618
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-060820/2619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1253. **CVE ID : CVE-2020-1310**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when Component Object Model (COM) client uses special case IIDs, aka 'Component Object Model Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1311**	N/A	O-MIC-WIND-060820/2620
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server fails to properly handle messages sent from TSF clients, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1314**	N/A	O-MIC-WIND-060820/2621
Information Exposure	09-06-2020	2.6	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory, aka 'Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1315**	N/A	O-MIC-WIND-060820/2622
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-060820/2623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306. **CVE ID : CVE-2020-1334**		
Information Exposure	09-06-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1348**	N/A	O-MIC-WIND-060820/2624
windows_server_2016					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0916. **CVE ID : CVE-2020-0915**	N/A	O-MIC-WIND-060820/2625
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0915. **CVE ID : CVE-2020-0916**	N/A	O-MIC-WIND-060820/2626
Improper Privilege	09-06-2020	7.2	An elevation of privilege vulnerability exists in	N/A	O-MIC-WIND-060820/2627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170. **CVE ID : CVE-2020-1163**		
Improper Input Validation	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Shell does not properly validate file paths.An attacker who successfully exploited this vulnerability could run arbitrary code in the context of the current user, aka 'Windows Shell Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1286**	N/A	O-MIC-WIND-060820/2628
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1294. **CVE ID : CVE-2020-1287**	N/A	O-MIC-WIND-060820/2629
Improper Privilege Management	09-06-2020	9	An elevation of privilege vulnerability exists when Group Policy improperly	N/A	O-MIC-WIND-060820/2630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1317**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-0986**	N/A	O-MIC-WIND-060820/2631
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1073**	N/A	O-MIC-WIND-060820/2632
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1160**	N/A	O-MIC-WIND-060820/2633
Improper Privilege	09-06-2020	4.6	An elevation of privilege (user to user) vulnerability	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			exists in Windows Security Health Service when handling certain objects in memory.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1324. **CVE ID : CVE-2020-1162**		060820/2634
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163. **CVE ID : CVE-2020-1170**	N/A	O-MIC-WIND-060820/2635
Improper Input Validation	09-06-2020	4.9	A denial of service vulnerability exists when Windows Registry improperly handles filesystem operations, aka 'Windows Registry Denial of Service Vulnerability'. **CVE ID : CVE-2020-1194**	N/A	O-MIC-WIND-060820/2636
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the printconfig.dll handles objects in memory, aka 'Windows Print	N/A	O-MIC-WIND-060820/2637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Configuration Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1196**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1197**	N/A	O-MIC-WIND-060820/2638
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way the Windows Now Playing Session Manager handles objects in memory, aka 'Windows Now Playing Session Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1201**	N/A	O-MIC-WIND-060820/2639
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1203. **CVE ID : CVE-2020-1202**	N/A	O-MIC-WIND-060820/2640
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to	N/A	O-MIC-WIND-060820/2641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properly handle objects in memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1202. **CVE ID : CVE-2020-1203**		
Improper Privilege Management	09-06-2020	3.6	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1204**	N/A	O-MIC-WIND-060820/2642
Information Exposure	09-06-2020	5	An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1206**	N/A	O-MIC-WIND-060820/2643
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1247, CVE-2020-1251,	N/A	O-MIC-WIND-060820/2644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1207**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1236. **CVE ID : CVE-2020-1208**	N/A	O-MIC-WIND-060820/2645
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Network List Service handles objects in memory, aka 'Windows Network List Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1209**	N/A	O-MIC-WIND-060820/2646
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1211**	N/A	O-MIC-WIND-060820/2647
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when an OLE Automation component improperly handles memory.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-060820/2648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution on the victim system, aka 'OLE Automation Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1212**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1213**	N/A	O-MIC-WIND-060820/2649
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1214**	N/A	O-MIC-WIND-060820/2650
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1215**	N/A	O-MIC-WIND-060820/2651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1216**	N/A	O-MIC-WIND-060820/2652
Information Exposure	09-06-2020	6.8	An information disclosure vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1217**	N/A	O-MIC-WIND-060820/2653
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1219**	N/A	O-MIC-WIND-060820/2654
URL Redirection to Untrusted Site ('Open Redirect')	09-06-2020	5.8	A spoofing vulnerability exists when theMicrosoft Edge (Chromium-based) in IE Mode improperly handles specific redirects, aka 'Microsoft Edge (Chromium-based) in IE Mode Spoofing Vulnerability'. **CVE ID : CVE-2020-1220**	N/A	O-MIC-WIND-060820/2655
Improper Privilege	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Microsoft Store Runtime	N/A	O-MIC-WIND-060820/2656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Microsoft Store Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1309. **CVE ID : CVE-2020-1222**		
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1260. **CVE ID : CVE-2020-1230**	N/A	O-MIC-WIND-060820/2657
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1231**	N/A	O-MIC-WIND-060820/2658
Out-of-bounds Read	09-06-2020	4.3	An information disclosure vulnerability exists when Media Foundation improperly handles objects	N/A	O-MIC-WIND-060820/2659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in memory, aka 'Media Foundation Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1232**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1233**	N/A	O-MIC-WIND-060820/2660
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when Windows Error Reporting improperly handles objects in memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1234**	N/A	O-MIC-WIND-060820/2661
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1265, CVE-2020-	N/A	O-MIC-WIND-060820/2662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1235**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1208. **CVE ID : CVE-2020-1236**	N/A	O-MIC-WIND-060820/2663
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1237**	N/A	O-MIC-WIND-060820/2664
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1239.	N/A	O-MIC-WIND-060820/2665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1238		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1238. **CVE ID : CVE-2020-1239**	N/A	O-MIC-WIND-060820/2666
Improper Input Validation	09-06-2020	6.8	A security feature bypass vulnerability exists when Windows Kernel fails to properly sanitize certain parameters.To exploit the vulnerability, a locally-authenticated attacker could attempt to run a specially crafted application on a targeted system.The update addresses the vulnerability by correcting how Windows Kernel handles parameter sanitization., aka 'Windows Kernel Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1241**	N/A	O-MIC-WIND-060820/2667
N/A	09-06-2020	5.8	A denial of service vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-1120.	N/A	O-MIC-WIND-060820/2668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1244		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1246**	N/A	O-MIC-WIND-060820/2669
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1247**	N/A	O-MIC-WIND-060820/2670
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1248**	N/A	O-MIC-WIND-060820/2671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1251**	N/A	O-MIC-WIND-060820/2672
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1310. **CVE ID : CVE-2020-1253**	N/A	O-MIC-WIND-060820/2673
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when Windows Modules Installer Service improperly handles class object members.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Modules Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1254**	N/A	O-MIC-WIND-060820/2674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	09-06-2020	6.5	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1255**	N/A	O-MIC-WIND-060820/2675
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1278, CVE-2020-1293. **CVE ID : CVE-2020-1257**	N/A	O-MIC-WIND-060820/2676
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1258**	N/A	O-MIC-WIND-060820/2677
Insufficiently Protected Credentials	09-06-2020	4	A security feature bypass vulnerability exists when Windows Host Guardian Service improperly handles hashes recorded and logged, aka 'Windows Host Guardian Service Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1259**	N/A	O-MIC-WIND-060820/2678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230. **CVE ID : CVE-2020-1260**	N/A	O-MIC-WIND-060820/2679
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1263. **CVE ID : CVE-2020-1261**	N/A	O-MIC-WIND-060820/2680
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1262**	N/A	O-MIC-WIND-060820/2681
Information	09-06-2020	2.1	An information disclosure	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1261. **CVE ID : CVE-2020-1263**		060820/2682
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1264**	N/A	O-MIC-WIND-060820/2683
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1265**	N/A	O-MIC-WIND-060820/2684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1266**	N/A	O-MIC-WIND-060820/2685
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when a Windows service improperly handles objects in memory, aka 'Windows Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1268**	N/A	O-MIC-WIND-060820/2686
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316.	N/A	O-MIC-WIND-060820/2687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1269		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the wlansvc.dll handles objects in memory, aka 'Windows WLAN Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1270**	N/A	O-MIC-WIND-060820/2688
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1271**	N/A	O-MIC-WIND-060820/2689
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1277, CVE-2020-1302, CVE-2020-1312. **CVE ID : CVE-2020-1272**	N/A	O-MIC-WIND-060820/2690
Improper	09-06-2020	4.6	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1273**		060820/2691
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1274**	N/A	O-MIC-WIND-060820/2692
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-	N/A	O-MIC-WIND-060820/2693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1275**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1276**	N/A	O-MIC-WIND-060820/2694
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1302, CVE-2020-1312. **CVE ID : CVE-2020-1277**	N/A	O-MIC-WIND-060820/2695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1293. **CVE ID : CVE-2020-1278**	N/A	O-MIC-WIND-060820/2696
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when Windows Lockscreen fails to properly load spotlight images from a secure location, aka 'Windows Lockscreen Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1279**	N/A	O-MIC-WIND-060820/2697
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Bluetooth Service handles objects in memory, aka 'Windows Bluetooth Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1280**	N/A	O-MIC-WIND-060820/2698
Improper Input Validation	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1281**	N/A	O-MIC-WIND-060820/2699
Improper Privilege	09-06-2020	6.8	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1282**		060820/2700
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.1	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2020-1283**	N/A	O-MIC-WIND-060820/2701
N/A	09-06-2020	4.3	A denial of service vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Denial of Service Vulnerability'. **CVE ID : CVE-2020-1284**	N/A	O-MIC-WIND-060820/2702
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1290**	N/A	O-MIC-WIND-060820/2703
Improper Privilege	09-06-2020	6.8	An elevation of privilege vulnerability exists in the	N/A	O-MIC-WIND-060820/2704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1291**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in OpenSSH for Windows when it does not properly restrict access to configuration settings, aka 'OpenSSH for Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1292**	N/A	O-MIC-WIND-060820/2705
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1278. **CVE ID : CVE-2020-1293**	N/A	O-MIC-WIND-060820/2706
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1287. **CVE ID : CVE-2020-1294**	N/A	O-MIC-WIND-060820/2707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	09-06-2020	2.1	A vulnerability exists in the way the Windows Diagnostics & feedback settings app handles objects in memory, aka 'Windows Diagnostics & feedback Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1296**	N/A	O-MIC-WIND-060820/2708
N/A	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1299**	N/A	O-MIC-WIND-060820/2709
N/A	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows fails to properly handle cabinet files.To exploit the vulnerability, an attacker would have to convince a user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.The update addresses the vulnerability by correcting how Windows handles cabinet files., aka 'Windows Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-060820/2710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1300		
N/A	09-06-2020	6.5	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1301**	N/A	O-MIC-WIND-060820/2711
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1277, CVE-2020-1312. **CVE ID : CVE-2020-1302**	N/A	O-MIC-WIND-060820/2712
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1304**	N/A	O-MIC-WIND-060820/2713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1305**	N/A	O-MIC-WIND-060820/2714
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1334. **CVE ID : CVE-2020-1306**	N/A	O-MIC-WIND-060820/2715
Improper Privilege Management	09-06-2020	9.3	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1316. **CVE ID : CVE-2020-1307**	N/A	O-MIC-WIND-060820/2716
Improper	09-06-2020	6.8	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists when the Microsoft Store Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Microsoft Store Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1222. **CVE ID : CVE-2020-1309**		060820/2717
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1253. **CVE ID : CVE-2020-1310**	N/A	O-MIC-WIND-060820/2718
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when Component Object Model (COM) client uses special case IIDs, aka 'Component Object Model Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1311**	N/A	O-MIC-WIND-060820/2719
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain	N/A	O-MIC-WIND-060820/2720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1277, CVE-2020-1302. **CVE ID : CVE-2020-1312**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Update Orchestrator Service improperly handles file operations, aka 'Windows Update Orchestrator Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1313**	N/A	O-MIC-WIND-060820/2721
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server fails to properly handle messages sent from TSF clients, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1314**	N/A	O-MIC-WIND-060820/2722
Information Exposure	09-06-2020	2.6	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory, aka 'Internet Explorer Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-060820/2723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1315		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307. **CVE ID : CVE-2020-1316**	N/A	O-MIC-WIND-060820/2724
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege (user to user) vulnerability exists in Windows Security Health Service when handling certain objects in memory.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1162. **CVE ID : CVE-2020-1324**	N/A	O-MIC-WIND-060820/2725
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233,	N/A	O-MIC-WIND-060820/2726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306. **CVE ID : CVE-2020-1334**		
Information Exposure	09-06-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1348**	N/A	O-MIC-WIND-060820/2727
windows_server_2019					
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0916. **CVE ID : CVE-2020-0915**	N/A	O-MIC-WIND-060820/2728
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0915. **CVE ID : CVE-2020-0916**	N/A	O-MIC-WIND-060820/2729
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that	N/A	O-MIC-WIND-060820/2730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170. **CVE ID : CVE-2020-1163**		
Improper Input Validation	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Shell does not properly validate file paths.An attacker who successfully exploited this vulnerability could run arbitrary code in the context of the current user, aka 'Windows Shell Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1286**	N/A	O-MIC-WIND-060820/2731
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1294. **CVE ID : CVE-2020-1287**	N/A	O-MIC-WIND-060820/2732
Improper Privilege Management	09-06-2020	9	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group	N/A	O-MIC-WIND-060820/2733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1317**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-0986**	N/A	O-MIC-WIND-060820/2734
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1073**	N/A	O-MIC-WIND-060820/2735
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1160**	N/A	O-MIC-WIND-060820/2736
Improper Privilege	09-06-2020	4.6	An elevation of privilege (user to user) vulnerability exists in Windows Security	N/A	O-MIC-WIND-060820/2737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Health Service when handling certain objects in memory.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1324. **CVE ID : CVE-2020-1162**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163. **CVE ID : CVE-2020-1170**	N/A	O-MIC-WIND-060820/2738
Improper Input Validation	09-06-2020	4.9	A denial of service vulnerability exists when Windows Registry improperly handles filesystem operations, aka 'Windows Registry Denial of Service Vulnerability'. **CVE ID : CVE-2020-1194**	N/A	O-MIC-WIND-060820/2739
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the printconfig.dll handles objects in memory, aka 'Windows Print Configuration Elevation of	N/A	O-MIC-WIND-060820/2740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. **CVE ID : CVE-2020-1196**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1197**	N/A	O-MIC-WIND-060820/2741
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the way the Windows Now Playing Session Manager handles objects in memory, aka 'Windows Now Playing Session Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1201**	N/A	O-MIC-WIND-060820/2742
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1203. **CVE ID : CVE-2020-1202**	N/A	O-MIC-WIND-060820/2743
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in	N/A	O-MIC-WIND-060820/2744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1202. **CVE ID : CVE-2020-1203**		
Improper Privilege Management	09-06-2020	3.6	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1204**	N/A	O-MIC-WIND-060820/2745
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1247, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1207**	N/A	O-MIC-WIND-060820/2746
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-060820/2747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2020-1236. **CVE ID : CVE-2020-1208**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1211**	N/A	O-MIC-WIND-060820/2748
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when an OLE Automation component improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'OLE Automation Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1212**	N/A	O-MIC-WIND-060820/2749
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1213**	N/A	O-MIC-WIND-060820/2750
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory,	N/A	O-MIC-WIND-060820/2751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1214**		
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1216, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1215**	N/A	O-MIC-WIND-060820/2752
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1230, CVE-2020-1260. **CVE ID : CVE-2020-1216**	N/A	O-MIC-WIND-060820/2753
Information Exposure	09-06-2020	6.8	An information disclosure vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1217**	N/A	O-MIC-WIND-060820/2754
Improper Restriction	09-06-2020	7.6	A remote code execution vulnerability exists in the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1219**		060820/2755
URL Redirection to Untrusted Site ('Open Redirect')	09-06-2020	5.8	A spoofing vulnerability exists when theMicrosoft Edge (Chromium-based) in IE Mode improperly handles specific redirects, aka 'Microsoft Edge (Chromium-based) in IE Mode Spoofing Vulnerability'. **CVE ID : CVE-2020-1220**	N/A	O-MIC-WIND-060820/2756
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Microsoft Store Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Microsoft Store Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1309. **CVE ID : CVE-2020-1222**	N/A	O-MIC-WIND-060820/2757
N/A	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1260.	N/A	O-MIC-WIND-060820/2758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1230		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1231**	N/A	O-MIC-WIND-060820/2759
Out-of-bounds Read	09-06-2020	4.3	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1232**	N/A	O-MIC-WIND-060820/2760
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1233**	N/A	O-MIC-WIND-060820/2761
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when Windows Error Reporting improperly handles objects	N/A	O-MIC-WIND-060820/2762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1234**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1235**	N/A	O-MIC-WIND-060820/2763
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1208. **CVE ID : CVE-2020-1236**	N/A	O-MIC-WIND-060820/2764
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-060820/2765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2020-0986, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1237**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1239. **CVE ID : CVE-2020-1238**	N/A	O-MIC-WIND-060820/2766
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1238. **CVE ID : CVE-2020-1239**	N/A	O-MIC-WIND-060820/2767
Improper Input Validation	09-06-2020	6.8	A security feature bypass vulnerability exists when Windows Kernel fails to properly sanitize certain parameters.To exploit the vulnerability, a locally-authenticated attacker could attempt to run a specially crafted application on a targeted system.The update	N/A	O-MIC-WIND-060820/2768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			addresses the vulnerability by correcting how Windows Kernel handles parameter sanitization., aka 'Windows Kernel Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1241**		
Information Exposure	09-06-2020	2.6	An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests, aka 'Microsoft Edge Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1242**	N/A	O-MIC-WIND-060820/2769
N/A	09-06-2020	5.8	A denial of service vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-1120. **CVE ID : CVE-2020-1244**	N/A	O-MIC-WIND-060820/2770
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-	N/A	O-MIC-WIND-060820/2771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1246**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1251, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1247**	N/A	O-MIC-WIND-060820/2772
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1253, CVE-2020-1310. **CVE ID : CVE-2020-1251**	N/A	O-MIC-WIND-060820/2773
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-060820/2774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1310. **CVE ID : CVE-2020-1253**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when Windows Modules Installer Service improperly handles class object members.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Modules Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1254**	N/A	O-MIC-WIND-060820/2775
Unrestricted Upload of File with Dangerous Type	09-06-2020	6.5	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1255**	N/A	O-MIC-WIND-060820/2776
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1278, CVE-2020-1293.	N/A	O-MIC-WIND-060820/2777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1257		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1258**	N/A	O-MIC-WIND-060820/2778
Insufficiently Protected Credentials	09-06-2020	4	A security feature bypass vulnerability exists when Windows Host Guardian Service improperly handles hashes recorded and logged, aka 'Windows Host Guardian Service Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1259**	N/A	O-MIC-WIND-060820/2779
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1213, CVE-2020-1214, CVE-2020-1215, CVE-2020-1216, CVE-2020-1230. **CVE ID : CVE-2020-1260**	N/A	O-MIC-WIND-060820/2780
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1263.	N/A	O-MIC-WIND-060820/2781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1261		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1262**	N/A	O-MIC-WIND-060820/2782
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1261. **CVE ID : CVE-2020-1263**	N/A	O-MIC-WIND-060820/2783
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-	N/A	O-MIC-WIND-060820/2784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1264**		
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1266**	N/A	O-MIC-WIND-060820/2785
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1269**	N/A	O-MIC-WIND-060820/2786
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in the way that the wlansvc.dll	N/A	O-MIC-WIND-060820/2787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handles objects in memory, aka 'Windows WLAN Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1270**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1271**	N/A	O-MIC-WIND-060820/2788
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1277, CVE-2020-1302, CVE-2020-1312. **CVE ID : CVE-2020-1272**	N/A	O-MIC-WIND-060820/2789
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows	N/A	O-MIC-WIND-060820/2790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1274**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1307, CVE-2020-1316. **CVE ID : CVE-2020-1276**	N/A	O-MIC-WIND-060820/2791
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-060820/2792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1272, CVE-2020-1302, CVE-2020-1312. **CVE ID : CVE-2020-1277**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1293. **CVE ID : CVE-2020-1278**	N/A	O-MIC-WIND-060820/2793
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when Windows Lockscreen fails to properly load spotlight images from a secure location, aka 'Windows Lockscreen Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1279**	N/A	O-MIC-WIND-060820/2794
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Bluetooth Service handles objects in memory, aka 'Windows Bluetooth Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1280**	N/A	O-MIC-WIND-060820/2795
Improper Input Validation	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution	N/A	O-MIC-WIND-060820/2796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1281**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1304, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1282**	N/A	O-MIC-WIND-060820/2797
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-06-2020	7.1	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2020-1283**	N/A	O-MIC-WIND-060820/2798
Information Exposure	09-06-2020	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1290**	N/A	O-MIC-WIND-060820/2799
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege	N/A	O-MIC-WIND-060820/2800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1291**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in OpenSSH for Windows when it does not properly restrict access to configuration settings, aka 'OpenSSH for Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1292**	N/A	O-MIC-WIND-060820/2801
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1257, CVE-2020-1278. **CVE ID : CVE-2020-1293**	N/A	O-MIC-WIND-060820/2802
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1287. **CVE ID : CVE-2020-1294**	N/A	O-MIC-WIND-060820/2803
Information Exposure	09-06-2020	2.1	A vulnerability exists in the way the Windows Diagnostics & feedback settings app handles objects in memory, aka 'Windows Diagnostics & feedback	N/A	O-MIC-WIND-060820/2804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1296**		
N/A	09-06-2020	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1299**	N/A	O-MIC-WIND-060820/2805
N/A	09-06-2020	6.8	A remote code execution vulnerability exists when Microsoft Windows fails to properly handle cabinet files.To exploit the vulnerability, an attacker would have to convince a user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.The update addresses the vulnerability by correcting how Windows handles cabinet files., aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1300**	N/A	O-MIC-WIND-060820/2806
N/A	09-06-2020	6.5	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0	N/A	O-MIC-WIND-060820/2807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(SMBv1) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1301**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1277, CVE-2020-1312. **CVE ID : CVE-2020-1302**	N/A	O-MIC-WIND-060820/2808
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1306, CVE-2020-1334. **CVE ID : CVE-2020-1304**	N/A	O-MIC-WIND-060820/2809
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka	N/A	O-MIC-WIND-060820/2810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows State Repository Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1305**		
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1334. **CVE ID : CVE-2020-1306**	N/A	O-MIC-WIND-060820/2811
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when the Microsoft Store Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Microsoft Store Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1222. **CVE ID : CVE-2020-1309**	N/A	O-MIC-WIND-060820/2812
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-060820/2813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2020-1207, CVE-2020-1247, CVE-2020-1251, CVE-2020-1253. **CVE ID : CVE-2020-1310**		
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists when Component Object Model (COM) client uses special case IIDs, aka 'Component Object Model Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1311**	N/A	O-MIC-WIND-060820/2814
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1272, CVE-2020-1277, CVE-2020-1302. **CVE ID : CVE-2020-1312**	N/A	O-MIC-WIND-060820/2815
Improper Privilege Management	09-06-2020	6.8	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server fails to properly handle messages sent from TSF clients, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-060820/2816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1314		
Information Exposure	09-06-2020	2.6	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory, aka 'Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1315**	N/A	O-MIC-WIND-060820/2817
Improper Privilege Management	09-06-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1307. **CVE ID : CVE-2020-1316**	N/A	O-MIC-WIND-060820/2818
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege (user to user) vulnerability exists in Windows Security Health Service when handling certain objects in memory.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1162. **CVE ID : CVE-2020-1324**	N/A	O-MIC-WIND-060820/2819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1231, CVE-2020-1233, CVE-2020-1235, CVE-2020-1265, CVE-2020-1282, CVE-2020-1304, CVE-2020-1306. **CVE ID : CVE-2020-1334**	N/A	O-MIC-WIND-060820/2820
Information Exposure	09-06-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1348**	N/A	O-MIC-WIND-060820/2821
azure_devops_server					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-06-2020	4.3	A spoofing vulnerability exists in Microsoft Azure DevOps Server when it fails to properly handle web requests, aka 'Azure DevOps Server HTML Injection Vulnerability'. **CVE ID : CVE-2020-1327**	N/A	O-MIC-AZUR-060820/2822
Mitsubishielectric					
melsec_iq-r16cpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/202	O-MIT-MELS-060820/2823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	0-001_en.pdf	
melsec_iq-r32cpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2824
melsec_iq-r120cpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2825
melsec_iq-r08fcpu_firmware					
Uncontrolled Resource	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware	https://www.mitsubish	O-MIT-MELS-060820/2826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	ielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	
melsec_iq-r16fcpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2827
melsec_iq-r32fcpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
melsec_iq-r120fcpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2829
melsec_iq-r08pcpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2830
melsec_iq-r16pcpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**		
melsec_iq-r32pcpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2832
melsec_iq-r120pcpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2833
melsec_iq-r08sfcpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/202	O-MIT-MELS-060820/2834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	0-001_en.pdf	
melsec_iq-r16sfcpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2835
melsec_iq-r32sfcpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2836
melsec_iq-r120sfcpu_firmware					
Uncontrolled Resource	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware	https://www.mitsubish	O-MIT-MELS-060820/2837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	ielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	
melsec_iq-rj71en71_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2838
melsec_iq-r00cpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
melsec_iq-r01cpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2840
melsec_iq-r02cpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2841
melsec_iq-r04cpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**		
melsec_iq-r08cpu_firmware					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	O-MIT-MELS-060820/2843
Opensuse					
leap					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	O-OPE-LEAP-060820/2844
Information Exposure	12-06-2020	3.6	A flaw was found in the Linux kernel's implementation of Userspace core dumps. This flaw allows an attacker with a local account to crash a trivial program and exfiltrate private kernel data. **CVE ID : CVE-2020-10732**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10732	O-OPE-LEAP-060820/2845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	6.9	A flaw was found in the Linux Kernel in versions after 4.5-rc1 in the way mremap handled DAX Huge Pages. This flaw allows a local attacker with access to a DAX enabled storage to escalate their privileges on the system. **CVE ID : CVE-2020-10757**	https://security.netapp.com/advisory/ntap-20200702-0004/	O-OPE-LEAP-060820/2846
Incorrect Permission Assignment for Critical Resource	08-06-2020	3.6	An issue was discovered in LinuxTV xawtv before 3.107. The function dev_open() in v4l-conf.c does not perform sufficient checks to prevent an unprivileged caller of the program from opening unintended filesystem paths. This allows a local attacker with access to the v4l-conf setuid-root program to test for the existence of arbitrary files and to trigger an open on arbitrary files with mode O_RDWR. To achieve this, relative path components need to be added to the device path, as demonstrated by a v4l-conf -c /dev/../root/.bash_history command. **CVE ID : CVE-2020-13696**	http://www.openwall.com/lists/oss-security/2020/06/04/6	O-OPE-LEAP-060820/2847
Paloaltonetworks					
pan-os					
Out-of-bounds Write	10-06-2020	9	A buffer overflow vulnerability in the authd component of the PAN-OS management server allows authenticated	N/A	O-PAL-PAN--060820/2848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrators to disrupt system processes and potentially execute arbitrary code with root privileges. This issue affects: All versions of PAN-OS 7.1 and PAN-OS 8.0; PAN-OS 8.1 versions earlier than PAN-OS 8.1.13; PAN-OS 9.0 versions earlier than PAN-OS 9.0.7. **CVE ID : CVE-2020-2027**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-06-2020	9	An OS Command Injection vulnerability in PAN-OS management server allows authenticated administrators to execute arbitrary OS commands with root privileges when uploading a new certificate in FIPS-CC mode. This issue affects: All versions of PAN-OS 7.1 and PAN-OS 8.0; PAN-OS 8.1 versions earlier than PAN-OS 8.1.13; PAN-OS 9.0 versions earlier than PAN-OS 9.0.7. **CVE ID : CVE-2020-2028**	N/A	O-PAL-PAN--060820/2849
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-06-2020	9	An OS Command Injection vulnerability in the PAN-OS web management interface allows authenticated administrators to execute arbitrary OS commands with root privileges by sending a malicious request to generate new certificates for use in the PAN-OS configuration. This issue affects: All versions of PAN-OS 8.0; PAN-OS 7.1 versions	N/A	O-PAL-PAN--060820/2850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than PAN-OS 7.1.26; PAN-OS 8.1 versions earlier than PAN-OS 8.1.13. **CVE ID : CVE-2020-2029**		
Qualcomm					
qca6574au_firmware					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCA6-060820/2851
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-QCA6-060820/2852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	lletins/may-2020-bulletin	
qcs405_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCS4-060820/2853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCS4-060820/2854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCS4-060820/2855
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may	O-QUA-QCS4-060820/2856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	-2020-bulletin	
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCS4-060820/2857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
ipq8074_firmware					
Use After Free	02-06-2020	7.2	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081, SC8180X, SXR2130 **CVE ID : CVE-2020-3618**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-IPQ8-060820/2858
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-IPQ8-060820/2859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
qca6174a_firmware					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCA6-060820/2860
qca9377_firmware					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	O-QUA-QCA9-060820/2861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	bulletin	
qca9379_firmware					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCA9-060820/2862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
sdm429w_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/2863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/2864
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	O-QUA-SDM4-060820/2865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	bulletin	
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/2866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/2867
sc7180_firmware					
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SC71-060820/2868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
apq8009_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3610**		
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2870
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2873
Time-of-check Time-of-use (TOCTOU)	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto,	https://www.qualcomm.com/company/produ	O-QUA-APQ8-060820/2874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Race Condition			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	ct-security/bulletins/may-2020-bulletin	
apq8098_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2876
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2879
msm8953_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	m.com/company/product-security/bulletins/may-2020-bulletin	060820/2880
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2883
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2885
msm8998_firmware					
Improper Restriction	02-06-2020	4.6	Possibility of out of bound access while processing the	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	m.com/company/product-security/bulletins/may-2020-bulletin	060820/2886
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
nicobar_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-NICO-060820/2889
Improper Restriction of Operations	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon	https://www.qualcomm.com/company/produ	O-QUA-NICO-060820/2890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	ct-security/bulletins/may-2020-bulletin	
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-NICO-060820/2891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
apq8053_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2893
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2896
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-APQ8-060820/2897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	lletins/may-2020-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mdm9207c_firmware					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2899
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2902
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
msm8905_firmware					
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2905
qcn7605_firmware					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some	https://www.qualcomm.com/com	O-QUA-QCN7-060820/2906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	pany/product-security/bulletins/may-2020-bulletin	
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCN7-060820/2907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
sdm845_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM8-060820/2908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM8-060820/2909
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM8-060820/2910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM8-060820/2911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM8-060820/2912
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM8-060820/2913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM8-060820/2914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM8-060820/2915
apq8017_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
apq8096au_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2917
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some	https://www.qualcomm.com/com	O-QUA-APQ8-060820/2918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	pany/product-security/bulletins/may-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2920
Improper	02-06-2020	10	Array out of bound may	https://ww	O-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	w.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	060820/2921
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-APQ8-060820/2922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
sda845_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDA8-060820/2923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDA8-060820/2924
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDA8-060820/2925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
sdm636_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2927
Buffer Copy without Checking Size of Input ('Classic Buffer	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDM6-060820/2928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	lletins/may-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2930
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper	https://www.qualcomm.com/com	O-QUA-SDM6-060820/2931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	pany/product-security/bulletins/may-2020-bulletin	
sdm670_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2934
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more	https://www.qualcomm.com/company/produ	O-QUA-SDM6-060820/2935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	ct-security/bulletins/may-2020-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2936
sdm710_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM7-060820/2937
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM7-060820/2938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM7-060820/2939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM7-060820/2940
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDM7-060820/2941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	lletins/may-2020-bulletin	
sm6150_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM61-060820/2942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM61-060820/2943
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM61-060820/2944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM61-060820/2945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM61-060820/2946
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in	https://www.qualcomm.com/company/product-	O-QUA-SM61-060820/2947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	security/bulletins/may-2020-bulletin	
qm215_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QM21-060820/2948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QM21-060820/2949
Improper Restriction of Operations	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon	https://www.qualcomm.com/company/produ	O-QUA-QM21-060820/2950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	ct-security/bulletins/may-2020-bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QM21-060820/2951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QM21-060820/2952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QM21-060820/2953
qca8081_firmware					
Use After Free	02-06-2020	7.2	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081, SC8180X, SXR2130 **CVE ID : CVE-2020-3618**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCA8-060820/2954
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may	O-QUA-QCA8-060820/2955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	-2020-bulletin	
qcs404_firmware					
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCS4-060820/2956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
sm8150_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM81-060820/2957
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending	https://www.qualcomm.com/company/produ	O-QUA-SM81-060820/2958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	ct-security/bulletins/may-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM81-060820/2959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM81-060820/2960
Improper Validation of	02-06-2020	10	Array out of bound may occur while playing mp3 file	https://www.qualcom	O-QUA-SM81-060820/2961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	m.com/company/product-security/bulletins/may-2020-bulletin	
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM81-060820/2962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM81-060820/2963
mdm9206_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2964
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2967
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
mdm9607_firmware					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2970
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2973
mdm9650_firmware					
Reachable	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if	https://www.qualcom	O-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	m.com/company/product-security/bulletins/may-2020-bulletin	060820/2974
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/2975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
msm8996au_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2977
Buffer Copy without Checking Size of Input ('Classic	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-MSM8-060820/2978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	security/bulletins/may-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2980
Integer Overflow or	02-06-2020	10	Integer overflow may occur if atom size is less than atom	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	m.com/company/product-security/bulletins/may-2020-bulletin	060820/2981
sdm429_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/2982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/2983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/2984
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDM4-060820/2985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	lletins/may-2020-bulletin	
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/2986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/2987
sdm632_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2990
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDM6-060820/2991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	lletins/may-2020-bulletin	
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/2993
msm8917_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2996
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-MSM8-060820/2997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	lletins/may-2020-bulletin	
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/2999
msm8996_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/3000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
sdm450_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/3001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/3002
Improper Restriction of Operations	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon	https://www.qualcomm.com/company/produ	O-QUA-SDM4-060820/3003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	ct-security/bulletins/may-2020-bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/3004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/3005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/3006
sm8250_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM82-060820/3007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Improper Input Validation	02-06-2020	7.2	kernel failure due to load failures while running v1 path directly via kernel in Snapdragon Mobile in SM8250, SXR2130 **CVE ID : CVE-2020-3623**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM82-060820/3008
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	When making query to DSP capabilities, Stack out of bounds occurs due to wrong buffer length configured for DSP attributes in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in SM8250, SXR2130 **CVE ID : CVE-2020-3625**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM82-060820/3009
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	O-QUA-SM82-060820/3010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM82-060820/3011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM82-060820/3012
sxr2130_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SXR2-060820/3013
Use After Free	02-06-2020	7.2	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SXR2-060820/3014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SXR2130 **CVE ID : CVE-2020-3618**		
Improper Input Validation	02-06-2020	7.2	kernel failure due to load failures while running v1 path directly via kernel in Snapdragon Mobile in SM8250, SXR2130 **CVE ID : CVE-2020-3623**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SXR2-060820/3015
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	When making query to DSP capabilities, Stack out of bounds occurs due to wrong buffer length configured for DSP attributes in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in SM8250, SXR2130 **CVE ID : CVE-2020-3625**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SXR2-060820/3016
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SXR2-060820/3017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SXR2-060820/3018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3633		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SXR2-060820/3019
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SXR2-060820/3020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
sa6155p_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SA61-060820/3021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SA61-060820/3022
sc8180x_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL	https://www.qualcomm.com/company/produ	O-QUA-SC81-060820/3023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	ct-security/bulletins/may-2020-bulletin	
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SC81-060820/3024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Use After Free	02-06-2020	7.2	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081, SC8180X, SXR2130 **CVE ID : CVE-2020-3618**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SC81-060820/3025
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SC81-060820/3026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SC81-060820/3027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3645		
sdm850_firmware					
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM8-060820/3028
qcm2150_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCM2-060820/3029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCM2-060820/3030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
sdx55_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDX5-060820/3031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDX5-060820/3032
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDX5-060820/3033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
sda660_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDA6-060820/3034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDA6-060820/3035
Improper Restriction of Operations within the Bounds of a	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDA6-060820/3036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	lletins/may-2020-bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDA6-060820/3037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDA6-060820/3038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3641		
sdm439_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/3039
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may	O-QUA-SDM4-060820/3040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/3041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/3042
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in	https://www.qualcomm.com/company/produ	O-QUA-SDM4-060820/3043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	ct-security/bulletins/may-2020-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM4-060820/3044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3680**		
sdm630_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/3045
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDM6-060820/3046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	lletins/may-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/3047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/3048
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer	https://www.qualcomm.com/company/produ	O-QUA-SDM6-060820/3049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	ct-security/bulletins/may-2020-bulletin	
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/3050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
sdm660_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/3051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/3052
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/3053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/3054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDM6-060820/3055
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may	O-QUA-SDM6-060820/3056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	-2020-bulletin	
mdm9150_firmware					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/3057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/3058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3630		
mdm9640_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MDM9-060820/3059
msm8909w_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no	https://www.qualcomm.com/company/product-	O-QUA-MSM8-060820/3060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	security/bulletins/may-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/3061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/3062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3630		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/3063
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/3064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-MSM8-060820/3065
qcs605_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL	https://www.qualcomm.com/company/produ	O-QUA-QCS6-060820/3066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	ct-security/bulletins/may-2020-bulletin	
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCS6-060820/3067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCS6-060820/3068
Improper Restriction of	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video	https://www.qualcomm.com/com	O-QUA-QCS6-060820/3069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	pany/product-security/bulletins/may-2020-bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCS6-060820/3070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCS6-060820/3071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCS6-060820/3072
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCS6-060820/3073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**		
sdx20_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDX2-060820/3074
Reachable	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if	https://www.qualcom	O-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	m.com/company/product-security/bulletins/may-2020-bulletin	060820/3075
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDX2-060820/3076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDX2-060820/3077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDX2-060820/3078
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDX2-060820/3079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
sm7150_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM71-060820/3080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM71-060820/3081
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM71-060820/3082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM71-060820/3083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SM71-060820/3084
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted	https://www.qualcom	O-QUA-SM71-060820/3085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	m.com/company/product-security/bulletins/may-2020-bulletin	
sxr1130_firmware					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SXR1-060820/3086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SXR1-060820/3087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SXR1-060820/3088
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SXR1-060820/3089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**		
sdx24_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDX2-060820/3090
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some	https://www.qualcomm.com/com	O-QUA-SDX2-060820/3091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	pany/product-security/bulletins/may-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDX2-060820/3092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SDX2-060820/3093
rennell_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object	https://www.qualcomm.com/company/product-security/bu	O-QUA-RENN-060820/3094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	lletins/may-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-RENN-060820/3095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-RENN-060820/3096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-RENN-060820/3097
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-RENN-060820/3098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
sa415m_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SA41-060820/3099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SA41-060820/3100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SA41-060820/3101
saipan_firmware					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SAIP-060820/3102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SAIP-060820/3103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SAIP-060820/3104
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-SAIP-060820/3105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
ipq6018_firmware					
Use After Free	02-06-2020	7.2	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081, SC8180X, SXR2130 **CVE ID : CVE-2020-3618**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-IPQ6-060820/3106
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-IPQ6-060820/3107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
kamorta_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-KAMO-060820/3108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-KAMO-060820/3109
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in	https://www.qualcomm.com/company/produ	O-QUA-KAMO-060820/3110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	ct-security/bulletins/may-2020-bulletin	
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-KAMO-060820/3111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
qca6390_firmware					
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	O-QUA-QCA6-060820/3112
Realtek					
adsl_router_soc_firmware					
N/A	08-06-2020	6.5	A security misconfiguration vulnerability exists in the SDK of some Realtek	N/A	O-REA-ADSL-060820/3113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ADSL/PON Modem SoC firmware, which allows attackers using a default password to execute arbitrary commands remotely via the build-in network monitoring tool. **CVE ID : CVE-2020-12773**		
Redhat					
enterprise_linux					
Information Exposure	12-06-2020	3.6	A flaw was found in the Linux kernel's implementation of Userspace core dumps. This flaw allows an attacker with a local account to crash a trivial program and exfiltrate private kernel data. **CVE ID : CVE-2020-10732**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10732	O-RED-ENTE-060820/3114
N/A	03-06-2020	6	A vulnerability was found in all versions of containernetworking/plugins before version 0.8.6, that allows malicious containers in Kubernetes clusters to perform man-in-the-middle (MitM) attacks. A malicious container can exploit this flaw by sending rogue IPv6 router advertisements to the host or other containers, to redirect traffic to the malicious container. **CVE ID : CVE-2020-10749**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10749	O-RED-ENTE-060820/3115
Improper Privilege Management	09-06-2020	6.9	A flaw was found in the Linux Kernel in versions after 4.5-rc1 in the way mremap handled DAX Huge Pages. This flaw allows a	https://security.netapp.com/advisory/ntap-20200702-	O-RED-ENTE-060820/3116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local attacker with access to a DAX enabled storage to escalate their privileges on the system. **CVE ID : CVE-2020-10757**	0004/	
Reachable Assertion	09-06-2020	4	An assertion failure issue was found in the Network Block Device(NBD) Server in all QEMU versions before QEMU 5.0.1. This flaw occurs when an nbd-client sends a spec-compliant request that is near the boundary of maximum permitted request length. A remote nbd-client could use this flaw to crash the qemu-nbd server resulting in a denial of service. **CVE ID : CVE-2020-10761**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10761	O-RED-ENTE-060820/3117
sane-project					
sane_backends					
NULL Pointer Dereference	01-06-2020	2.1	A NULL pointer dereference in sanei_epson_net_read in SANE Backends before 1.0.30 allows a malicious device connected to the same local network as the victim to cause a denial of service, aka GHSL-2020-075. **CVE ID : CVE-2020-12867**	https://alioth-lists.debian.net/pipermail/sane-announce/2020/000041.html, https://gitlab.com/sane-project/backends/-/issues/279#issue-1-ghsl-2020-075-null-	O-SAN-SANE-060820/3118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pointer-dereference-in-sanei_epson_net_read	
Siemens					
simatic_s7-150_firmware					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14	N/A	O-SIE-SIMA-060820/3119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
logo\!_8_bm_firmware					
Missing Authenticati on for Critical Function	10-06-2020	6.4	A vulnerability has been identified in LOGO!8 BM (incl. SIPLUS variants) (All versions). The vulnerability could lead to an attacker reading and modifying the device configuration and obtain project files from affected devices. The security vulnerability could be exploited by an unauthenticated attacker with network access to port 135/tcp. No user interaction	N/A	O-SIE-LOGO-060820/3120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is required to exploit this security vulnerability. The vulnerability impacts confidentiality, integrity, and availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known. **CVE ID : CVE-2020-7589**		
sokkia					
gnr5_vanguard_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-06-2020	7.5	SOKKIA GNR5 Vanguard WEB version 1.2 (build: 91f2b2c3a04d203d79862f87e2440cb7cefc3cd3) and hardware version 212 allows remote attackers to bypass admin authentication via a SQL injection attack that uses the User Name or Password field on the login page. **CVE ID : CVE-2020-14054**	N/A	O-SOK-GNR5-060820/3121
Sony					
wf-1000x_firmware					
Missing Authentication for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing	N/A	O-SON-WF-1-060820/3122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			volume of the product. **CVE ID : CVE-2020-5589**		
wf-sp700n_firmware					
Missing Authenticati on for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	O-SON-WF-S-060820/3123
wh-1000xm2_firmware					
Missing Authenticati on for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	O-SON-WH-1-060820/3124
wh-1000xm3_firmware					
Missing Authenticati on for	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-	N/A	O-SON-WH-1-060820/3125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Function			1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**		
wh-ch700n_firmware					
Missing Authentication for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	O-SON-WH-C-060820/3126
wh-h900n_firmware					
Missing Authentication for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the	N/A	O-SON-WH-H-060820/3127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**		
wh-xb700_firmware					
Missing Authenticati on for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	O-SON-WH-X-060820/3128
wh-xb900n_firmware					
Missing Authenticati on for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	O-SON-WH-X-060820/3129
wi-1000x_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	O-SON-WI-1-060820/3130
wi-c600n_firmware					
Missing Authentication for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	O-SON-WI-C-060820/3131
wi-sp600n_firmware					
Missing Authentication for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with	N/A	O-SON-WI-S-060820/3132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**		
Trendnet					
tew-827dru_firmware					
Out-of-bounds Write	15-06-2020	6.5	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action kick_ban_wifi_mac_allow with a sufficiently long qcawifi.wifi0_vap0.maclist key. **CVE ID : CVE-2020-14074**	N/A	O-TRE-TEW--060820/3133
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	15-06-2020	9	TRENDnet TEW-827DRU devices through 2.06B04 contain multiple command injections in apply.cgi via the action pppoe_connect, ru_pppoe_connect, or dhcp_connect with the key wan_ifname (or wan0_dns), allowing an authenticated user to run arbitrary commands on the device. **CVE ID : CVE-2020-14075**	N/A	O-TRE-TEW--060820/3134
Out-of-bounds	15-06-2020	6.5	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer	N/A	O-TRE-TEW--060820/3135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action st_dev_connect, st_dev_disconnect, or st_dev_rconnect with a sufficiently long wan_type key. **CVE ID : CVE-2020-14076**		
Out-of-bounds Write	15-06-2020	6.5	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action set_sta_enrollee_pin_wifi1 (or set_sta_enrollee_pin_wifi0) with a sufficiently long wps_sta_enrollee_pin key. **CVE ID : CVE-2020-14077**	N/A	O-TRE-TEW--060820/3136
Out-of-bounds Write	15-06-2020	6.5	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action wifi_captive_portal_login with a sufficiently long REMOTE_ADDR key. **CVE ID : CVE-2020-14078**	N/A	O-TRE-TEW--060820/3137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	15-06-2020	6.5	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action auto_up_fw (or auto_up_lp) with a sufficiently long update_file_name key. **CVE ID : CVE-2020-14079**	N/A	O-TRE-TEW--060820/3138
Out-of-bounds Write	15-06-2020	7.5	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an unauthenticated user to execute arbitrary code by POSTing to apply_sec.cgi via the action ping_test with a sufficiently long ping_ipaddr key. **CVE ID : CVE-2020-14080**	N/A	O-TRE-TEW--060820/3139
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	15-06-2020	9	TRENDnet TEW-827DRU devices through 2.06B04 contain multiple command injections in apply.cgi via the action send_log_email with the key auth_acname (or auth_passwd), allowing an authenticated user to run arbitrary commands on the device. **CVE ID : CVE-2020-14081**	N/A	O-TRE-TEW--060820/3140
usavisionsys					
geovision_gv-as210_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	12-06-2020	10	GeoVision Door Access Control device family is hardcoded with a root password, which adopting an identical password in all devices. **CVE ID : CVE-2020-3928**	N/A	O-USA-GEOV-060820/3141
Inadequate Encryption Strength	12-06-2020	4.3	GeoVision Door Access Control device family employs shared cryptographic private keys for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext recover of encrypted messages. **CVE ID : CVE-2020-3929**	N/A	O-USA-GEOV-060820/3142
geovision_gv-as410_firmware					
Use of Hard-coded Credentials	12-06-2020	10	GeoVision Door Access Control device family is hardcoded with a root password, which adopting an identical password in all devices. **CVE ID : CVE-2020-3928**	N/A	O-USA-GEOV-060820/3143
Inadequate Encryption Strength	12-06-2020	4.3	GeoVision Door Access Control device family employs shared cryptographic private keys for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext recover of encrypted messages. **CVE ID : CVE-2020-3929**	N/A	O-USA-GEOV-060820/3144
geovision_gv-as810_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	12-06-2020	10	GeoVision Door Access Control device family is hardcoded with a root password, which adopting an identical password in all devices. **CVE ID : CVE-2020-3928**	N/A	O-USA-GEOV-060820/3145
Inadequate Encryption Strength	12-06-2020	4.3	GeoVision Door Access Control device family employs shared cryptographic private keys for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext recover of encrypted messages. **CVE ID : CVE-2020-3929**	N/A	O-USA-GEOV-060820/3146
geovision_gv-as1010_firmware					
Use of Hard-coded Credentials	12-06-2020	10	GeoVision Door Access Control device family is hardcoded with a root password, which adopting an identical password in all devices. **CVE ID : CVE-2020-3928**	N/A	O-USA-GEOV-060820/3147
Inadequate Encryption Strength	12-06-2020	4.3	GeoVision Door Access Control device family employs shared cryptographic private keys for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext recover of encrypted messages. **CVE ID : CVE-2020-3929**	N/A	O-USA-GEOV-060820/3148
geovision_gv-gf192x_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	12-06-2020	10	GeoVision Door Access Control device family is hardcoded with a root password, which adopting an identical password in all devices. **CVE ID : CVE-2020-3928**	N/A	O-USA-GEOV-060820/3149
Inadequate Encryption Strength	12-06-2020	4.3	GeoVision Door Access Control device family employs shared cryptographic private keys for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext recover of encrypted messages. **CVE ID : CVE-2020-3929**	N/A	O-USA-GEOV-060820/3150
Information Exposure	12-06-2020	2.1	GeoVision Door Access Control device family improperly stores and controls access to system logs, any users can read these logs. **CVE ID : CVE-2020-3930**	N/A	O-USA-GEOV-060820/3151
Wago					
pfc200_firmware					
Improper Privilege Management	11-06-2020	9	An exploitable code execution vulnerability exists in the Web-Based Management (WBM) functionality of WAGO PFC 200 03.03.10(15). A specially crafted series of HTTP requests can cause code execution resulting in remote code execution. An attacker can make an authenticated HTTP request	N/A	O-WAG-PFC2-060820/3152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to trigger this vulnerability. **CVE ID : CVE-2020-6090**		
zephyrproject					
zephyr					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-06-2020	5.8	Improper handling of the full-buffer case in the Zephyr Bluetooth implementation can result in memory corruption. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions, and version 1.14.0 and later versions. **CVE ID : CVE-2020-10061**	N/A	O-ZEP-ZEPH-060820/3153
Off-by-one Error	05-06-2020	7.5	An off-by-one error in the Zephyr project MQTT packet length decoder can result in memory corruption and possible remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions. **CVE ID : CVE-2020-10062**	N/A	O-ZEP-ZEPH-060820/3154
Integer Overflow or Wraparound	05-06-2020	5	A remote adversary with the ability to send arbitrary CoAP packets to be parsed by Zephyr is able to cause a denial of service. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions. **CVE ID : CVE-2020-10063**	N/A	O-ZEP-ZEPH-060820/3155
Improper Input Validation	05-06-2020	3.3	In the Zephyr project Bluetooth subsystem, certain duplicate and back-to-back packets can cause incorrect	N/A	O-ZEP-ZEPH-060820/3156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			behavior, resulting in a denial of service. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions, and version 1.14.0 and later versions. **CVE ID : CVE-2020-10068**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	In the Zephyr Project MQTT code, improper bounds checking can result in memory corruption and possibly remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions. **CVE ID : CVE-2020-10070**	N/A	O-ZEP-ZEPH-060820/3157
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	The Zephyr MQTT parsing code performs insufficient checking of the length field on publish messages, allowing a buffer overflow and potentially remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions. **CVE ID : CVE-2020-10071**	N/A	O-ZEP-ZEPH-060820/3158
ZTE					
f680_firmware					
Improper Input Validation	01-06-2020	3.3	ZTE's PON terminal product is impacted by the access control vulnerability. Due to the system not performing correct access control on some program interfaces, an attacker could use this	N/A	O-ZTE-F680-060820/3159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to tamper with the program interface parameters to perform unauthenticated operations. This affects: <ZTE F680><V9.0.10P1N6> **CVE ID : CVE-2020-6868**		
Hardware					
ARM					
cortex-a57					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	http://lists.llvm.org/pipermail/llvm-dev/2020-June/142109.html, https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/547520.html	H-ARM-CORT-060820/3160
cortex-a72					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow	http://lists.llvm.org/pipermail/llvm-dev/2020-June/14210	H-ARM-CORT-060820/3161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	9.html, https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/547520.html	
cortex-a73					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	http://lists.llvm.org/pipermail/llvm-dev/2020-June/142109.html, https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/54752	H-ARM-CORT-060820/3162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				0.html	
cortex-a34					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	http://lists.llvm.org/pipermail/llvm-dev/2020-June/142109.html, https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/547520.html	H-ARM-CORT-060820/3163
cortex-a32					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	http://lists.llvm.org/pipermail/llvm-dev/2020-June/142109.html, https://developer.arm.com/support/arm-security-updates/speculative-processor-	H-ARM-CORT-060820/3164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/547520.html	
cortex-a35					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	http://lists.llvm.org/pipermail/llvm-dev/2020-June/142109.html, https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/547520.html	H-ARM-CORT-060820/3165
cortex-a53					
Information Exposure	08-06-2020	2.1	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow unauthorized disclosure of	http://lists.llvm.org/pipermail/llvm-dev/2020-June/142109.html,	H-ARM-CORT-060820/3166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information to an attacker with local user access via a side-channel analysis, aka "straight-line speculation." **CVE ID : CVE-2020-13844**	https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability, https://gcc.gnu.org/pipermail/gcc-patches/2020-June/547520.html	
Asus					
rt-n11					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-ASU-RT-N-060820/3167
Broadcom					
adsl					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL	N/A	H-BRO-ADSL-060820/3168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
Canon					
selphy_cp1200					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-CAN-SELP-060820/3169
castel					
nextgen_dvr					
Improper Privilege Management	04-06-2020	6.5	Castel NextGen DVR v1.0.0 is vulnerable to privilege escalation through the Adminstrator/Users/Edit/:UserId functionality. Adminstrator/Users/Edit/:UserId fails to check that the request was submitted by an Administrator. This allows a normal user to escalate their privileges by adding additional roles to their account. **CVE ID : CVE-2020-11679**	N/A	H-CAS-NEXT-060820/3170
Incorrect Authorizatio	04-06-2020	4	Castel NextGen DVR v1.0.0 is vulnerable to authorization	N/A	H-CAS-NEXT-060820/3171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			bypass on all administrator functionality. The application fails to check that a request was submitted by an administrator. Consequently, a normal user can perform actions including, but not limited to, creating/modifying the file store, creating/modifying alerts, creating/modifying users, etc. **CVE ID : CVE-2020-11680**		
Insufficiently Protected Credentials	04-06-2020	4	Castel NextGen DVR v1.0.0 stores and displays credentials for the associated SMTP server in cleartext. Low privileged users can exploit this to create an administrator user and obtain the SMTP credentials. **CVE ID : CVE-2020-11681**	N/A	H-CAS-NEXT-060820/3172
Cross-Site Request Forgery (CSRF)	04-06-2020	4.3	Castel NextGen DVR v1.0.0 is vulnerable to CSRF in all state-changing request. A __RequestVerificationToken is set by the web interface, and included in requests sent by web interface. However, this token is not verified by the application: the token can be removed from all requests and the request will succeed. **CVE ID : CVE-2020-11682**	N/A	H-CAS-NEXT-060820/3173
Cisco					
isr_1101					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ISR_-060820/3174
isr_1109					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ISR_-060820/3175
isr_1111x					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto	N/A	H-CIS-ISR_-060820/3176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. **CVE ID : CVE-2020-3214**		
isr_111x					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ISR_-060820/3177
isr_1120					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ISR_-060820/3178
isr_1160					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient	N/A	H-CIS-ISR_-060820/3179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
isr_4431					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ISR_-060820/3180
isr_4461					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ISR_-060820/3181
nexus_1000v					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-060820/3182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3183
Improper Input Validation	03-06-2020	7.8	A vulnerability in Security Group Tag Exchange Protocol (SXP) in Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because crafted SXP packets are mishandled. An attacker	N/A	H-CIS-NEXU-060820/3184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending specifically crafted SXP packets to the affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3228**		
1120_connected_grid_router					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**	N/A	H-CIS-1120-060820/3185
1240_connected_grid_router					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid	N/A	H-CIS-1240-060820/3186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
1120					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3198**	N/A	H-CIS-1120-060820/3187
Improper Input Validation	03-06-2020	8.3	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid	N/A	H-CIS-1120-060820/3188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3199**		
Improper Input Validation	03-06-2020	8.3	A vulnerability in the implementation of the inter-VM channel of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, adjacent attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The vulnerability is due to insufficient validation of signaling packets that are destined to VDS. An attacker could exploit this vulnerability by sending malicious packets to an affected device. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. Because the device is	N/A	H-CIS-1120-060820/3189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			designed on a hypervisor architecture, exploitation of a vulnerability that affects the inter-VM channel may lead to a complete system compromise. For more information about this vulnerability, see the Details section of this advisory. **CVE ID : CVE-2020-3205**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in the image verification feature of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) could allow an authenticated, local attacker to boot a malicious software image on an affected device. The vulnerability is due to insufficient access restrictions on the area of code that manages the image verification feature. An attacker could exploit this vulnerability by first authenticating to the targeted device and then logging in to the Virtual Device Server (VDS) of an affected device. The attacker could then, from the VDS shell, disable Cisco IOS Software integrity (image) verification. A successful exploit could allow the attacker to boot a malicious Cisco IOS Software image on the targeted device. To exploit this vulnerability, the	N/A	H-CIS-1120-060820/3190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker must have valid user credentials at privilege level 15. **CVE ID : CVE-2020-3208**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the CLI parsers of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated, local attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The attacker must have valid user credentials at privilege level 15. The vulnerability is due to insufficient validation of arguments that are passed to specific VDS-related CLI commands. An attacker could exploit this vulnerability by authenticating to the targeted device and including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. **CVE ID : CVE-2020-3210**	N/A	H-CIS-1120-060820/3191
Improper Restriction	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco	N/A	H-CIS-1120-060820/3192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**		
Use of Hard-coded Credentials	03-06-2020	7.2	A vulnerability in the virtual console authentication of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated but low-privileged, local attacker to log in to the Virtual Device Server (VDS) of an affected device by using a set of default credentials. The vulnerability is due to the presence of weak, hard-coded credentials. An attacker could exploit this vulnerability by authenticating to the targeted device and then connecting to VDS through the device’s virtual console by using the static	N/A	H-CIS-1120-060820/3193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials. A successful exploit could allow the attacker to access the Linux shell of VDS as the root user. **CVE ID : CVE-2020-3234**		
1240					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3198**	N/A	H-CIS-1240-060820/3194
Improper Input Validation	03-06-2020	8.3	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more	N/A	H-CIS-1240-060820/3195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3199**		
Improper Input Validation	03-06-2020	8.3	A vulnerability in the implementation of the inter-VM channel of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, adjacent attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The vulnerability is due to insufficient validation of signaling packets that are destined to VDS. An attacker could exploit this vulnerability by sending malicious packets to an affected device. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. Because the device is designed on a hypervisor architecture, exploitation of a vulnerability that affects the inter-VM channel may lead to a complete system compromise. For more information about this vulnerability, see the Details	N/A	H-CIS-1240-060820/3196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2020-3205**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in the image verification feature of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) could allow an authenticated, local attacker to boot a malicious software image on an affected device. The vulnerability is due to insufficient access restrictions on the area of code that manages the image verification feature. An attacker could exploit this vulnerability by first authenticating to the targeted device and then logging in to the Virtual Device Server (VDS) of an affected device. The attacker could then, from the VDS shell, disable Cisco IOS Software integrity (image) verification. A successful exploit could allow the attacker to boot a malicious Cisco IOS Software image on the targeted device. To exploit this vulnerability, the attacker must have valid user credentials at privilege level 15. **CVE ID : CVE-2020-3208**	N/A	H-CIS-1240-060820/3197
Improper Neutralization of Special	03-06-2020	7.2	A vulnerability in the CLI parsers of Cisco IOS Software for Cisco 809 and	N/A	H-CIS-1240-060820/3198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated, local attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The attacker must have valid user credentials at privilege level 15. The vulnerability is due to insufficient validation of arguments that are passed to specific VDS-related CLI commands. An attacker could exploit this vulnerability by authenticating to the targeted device and including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. **CVE ID : CVE-2020-3210**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker	N/A	H-CIS-1240-060820/3199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**		
Use of Hard-coded Credentials	03-06-2020	7.2	A vulnerability in the virtual console authentication of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated but low-privileged, local attacker to log in to the Virtual Device Server (VDS) of an affected device by using a set of default credentials. The vulnerability is due to the presence of weak, hard-coded credentials. An attacker could exploit this vulnerability by authenticating to the targeted device and then connecting to VDS through the device’s virtual console by using the static credentials. A successful exploit could allow the attacker to access the Linux shell of VDS as the root user. **CVE ID : CVE-2020-3234**	N/A	H-CIS-1240-060820/3200
809					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3198**	N/A	H-CIS-809-060820/3201
Improper Input Validation	03-06-2020	8.3	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3199**	N/A	H-CIS-809-060820/3202
Improper	03-06-2020	8.3	A vulnerability in the	N/A	H-CIS-809-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			implementation of the inter-VM channel of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, adjacent attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The vulnerability is due to insufficient validation of signaling packets that are destined to VDS. An attacker could exploit this vulnerability by sending malicious packets to an affected device. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. Because the device is designed on a hypervisor architecture, exploitation of a vulnerability that affects the inter-VM channel may lead to a complete system compromise. For more information about this vulnerability, see the Details section of this advisory. **CVE ID : CVE-2020-3205**		060820/3203
Improper Privilege Management	03-06-2020	7.2	A vulnerability in the image verification feature of Cisco IOS Software for Cisco 809 and 829 Industrial	N/A	H-CIS-809-060820/3204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Integrated Services Routers (Industrial ISRs) could allow an authenticated, local attacker to boot a malicious software image on an affected device. The vulnerability is due to insufficient access restrictions on the area of code that manages the image verification feature. An attacker could exploit this vulnerability by first authenticating to the targeted device and then logging in to the Virtual Device Server (VDS) of an affected device. The attacker could then, from the VDS shell, disable Cisco IOS Software integrity (image) verification. A successful exploit could allow the attacker to boot a malicious Cisco IOS Software image on the targeted device. To exploit this vulnerability, the attacker must have valid user credentials at privilege level 15. **CVE ID : CVE-2020-3208**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the CLI parsers of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated, local attacker to execute arbitrary shell	N/A	H-CIS-809-060820/3205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands on the Virtual Device Server (VDS) of an affected device. The attacker must have valid user credentials at privilege level 15. The vulnerability is due to insufficient validation of arguments that are passed to specific VDS-related CLI commands. An attacker could exploit this vulnerability by authenticating to the targeted device and including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. **CVE ID : CVE-2020-3210**		
Use of Hard-coded Credentials	03-06-2020	7.2	A vulnerability in the virtual console authentication of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated but low-privileged, local attacker to log in to the Virtual Device Server (VDS) of an affected device by using a set of default credentials. The vulnerability is due to the presence of weak, hard-coded credentials. An	N/A	H-CIS-809-060820/3206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by authenticating to the targeted device and then connecting to VDS through the device’s virtual console by using the static credentials. A successful exploit could allow the attacker to access the Linux shell of VDS as the root user. **CVE ID : CVE-2020-3234**		
asr_1000-x					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ASR_-060820/3207
asr_1001					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device.	N/A	H-CIS-ASR_-060820/3208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3214		
asr_1002					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ASR_-060820/3209
asr_1004					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ASR_-060820/3210
asr_1006					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability	N/A	H-CIS-ASR_-060820/3211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
asr_1013					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ASR_-060820/3212
catalyst_c9404r					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3213
catalyst_c9407r					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level	N/A	H-CIS-CATA-060820/3214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
catalyst_c9410r					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3215
isr_1100					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ISR_-060820/3216
isr_422					
Improper	03-06-2020	7.2	A vulnerability in Cisco IOS	N/A	H-CIS-ISR_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		060820/3217
ws-c3650-12x48uq					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3218
ws-c3650-12x48ur					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device.	N/A	H-CIS-WS-C-060820/3219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3214		
ws-c3650-12x48uz					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3220
ws-c3650-24pd					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3221
ws-c3650-24pdm					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability	N/A	H-CIS-WS-C-060820/3222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
ws-c3650-24ps					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3223
ws-c3650-24td					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3224
ws-c3650-24ts					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level	N/A	H-CIS-WS-C-060820/3225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
ws-c3650-48fd					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3226
ws-c3650-48fq					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3227
ws-c3650-48fqm					
Improper	03-06-2020	7.2	A vulnerability in Cisco IOS	N/A	H-CIS-WS-C-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		060820/3228
ws-c3650-48fs					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3229
ws-c3650-48pd					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device.	N/A	H-CIS-WS-C-060820/3230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3214		
ws-c3650-48pq					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3231
ws-c3650-48ps					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3232
ws-c3650-48td					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability	N/A	H-CIS-WS-C-060820/3233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
ws-c3650-48tq					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3234
ws-c3650-48ts					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3235
ws-c3650-8x24uq					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level	N/A	H-CIS-WS-C-060820/3236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
ws-c3850-12s					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3237
829					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the	N/A	H-CIS-829-060820/3238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Details section of this advisory. **CVE ID : CVE-2020-3198**		
Improper Input Validation	03-06-2020	8.3	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3199**	N/A	H-CIS-829-060820/3239
Improper Input Validation	03-06-2020	8.3	A vulnerability in the implementation of the inter-VM channel of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, adjacent attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The vulnerability is due to insufficient validation of signaling packets that are	N/A	H-CIS-829-060820/3240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			destined to VDS. An attacker could exploit this vulnerability by sending malicious packets to an affected device. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. Because the device is designed on a hypervisor architecture, exploitation of a vulnerability that affects the inter-VM channel may lead to a complete system compromise. For more information about this vulnerability, see the Details section of this advisory. **CVE ID : CVE-2020-3205**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in the image verification feature of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) could allow an authenticated, local attacker to boot a malicious software image on an affected device. The vulnerability is due to insufficient access restrictions on the area of code that manages the image verification feature. An attacker could exploit this vulnerability by first authenticating to the targeted device and then logging in to the Virtual	N/A	H-CIS-829-060820/3241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Device Server (VDS) of an affected device. The attacker could then, from the VDS shell, disable Cisco IOS Software integrity (image) verification. A successful exploit could allow the attacker to boot a malicious Cisco IOS Software image on the targeted device. To exploit this vulnerability, the attacker must have valid user credentials at privilege level 15. **CVE ID : CVE-2020-3208**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the CLI parsers of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated, local attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The attacker must have valid user credentials at privilege level 15. The vulnerability is due to insufficient validation of arguments that are passed to specific VDS-related CLI commands. An attacker could exploit this vulnerability by authenticating to the targeted device and including malicious input as the argument of an affected	N/A	H-CIS-829-060820/3242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. **CVE ID : CVE-2020-3210**		
Use of Hard-coded Credentials	03-06-2020	7.2	A vulnerability in the virtual console authentication of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated but low-privileged, local attacker to log in to the Virtual Device Server (VDS) of an affected device by using a set of default credentials. The vulnerability is due to the presence of weak, hard-coded credentials. An attacker could exploit this vulnerability by authenticating to the targeted device and then connecting to VDS through the device’s virtual console by using the static credentials. A successful exploit could allow the attacker to access the Linux shell of VDS as the root user. **CVE ID : CVE-2020-3234**	N/A	H-CIS-829-060820/3243
nexus_3132q					
Authenticati on Bypass by	02-06-2020	5	Multiple products that implement the IP	N/A	H-CIS-NEXU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Spoofing			Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		060820/3244
nexus_3172					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3245
nexus_5548p					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could	N/A	H-CIS-NEXU-060820/3246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_5548up					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3247
nexus_5596t					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access	N/A	H-CIS-NEXU-060820/3248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_5596up					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3249
nexus_56128p					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nexus_5624q					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3251
nexus_5648q					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3252
nexus_5672up					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1)	N/A	H-CIS-NEXU-060820/3253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_5696q					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3254
nexus_6001					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent	N/A	H-CIS-NEXU-060820/3255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
Authenticati on Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network	N/A	H-CIS-NEXU-060820/3256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			behaviors. **CVE ID : CVE-2020-10136**		
nexus_6004					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**	N/A	H-CIS-NEXU-060820/3257
Authenticati on Bypass by	02-06-2020	5	Multiple products that implement the IP	N/A	H-CIS-NEXU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Spoofing			Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		060820/3258
nexus_7000_10-slot					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to	N/A	H-CIS-NEXU-060820/3259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
Improper Input Validation	03-06-2020	7.8	A vulnerability in Security Group Tag Exchange Protocol (SXP) in Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because crafted SXP packets are mishandled. An attacker could exploit this vulnerability by sending specifically crafted SXP packets to the affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3228**	N/A	H-CIS-NEXU-060820/3260
nexus_7000_18-slot					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE	N/A	H-CIS-NEXU-060820/3261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
Improper Input Validation	03-06-2020	7.8	A vulnerability in Security Group Tag Exchange Protocol (SXP) in Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. The	N/A	H-CIS-NEXU-060820/3262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because crafted SXP packets are mishandled. An attacker could exploit this vulnerability by sending specifically crafted SXP packets to the affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3228**		
nexus_7000_4-slot					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow,	N/A	H-CIS-NEXU-060820/3263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
Improper Input Validation	03-06-2020	7.8	A vulnerability in Security Group Tag Exchange Protocol (SXP) in Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because crafted SXP packets are mishandled. An attacker could exploit this vulnerability by sending specifically crafted SXP packets to the affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3228**	N/A	H-CIS-NEXU-060820/3264
nexus_7000_9-slot					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR	N/A	H-CIS-NEXU-060820/3265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
Improper Input Validation	03-06-2020	7.8	A vulnerability in Security Group Tag Exchange Protocol (SXP) in Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because	N/A	H-CIS-NEXU-060820/3266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted SXP packets are mishandled. An attacker could exploit this vulnerability by sending specifically crafted SXP packets to the affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3228**		
nexus_6004x					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the	N/A	H-CIS-NEXU-060820/3267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
nexus_7000					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3268
nexus_7700					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other	N/A	H-CIS-NEXU-060820/3269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected network behaviors. **CVE ID : CVE-2020-10136**		
catalyst_3650-12x48uq					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3270
catalyst_3650-12x48ur					
Improper Neutralization of Special Elements used in an OS Command ('OS	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying	N/A	H-CIS-CATA-060820/3271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
catalyst_3650-12x48uz					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided	N/A	H-CIS-CATA-060820/3272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
catalyst_3650-24pd					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3273
catalyst_3650-24pdm					
Improper Neutralizatio	03-06-2020	7.2	A vulnerability in the processing of boot options of	N/A	H-CIS-CATA-060820/3274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
catalyst_3650-48fq					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing	N/A	H-CIS-CATA-060820/3275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
catalyst_3650-48fqm					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges.	N/A	H-CIS-CATA-060820/3276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3207		
catalyst_3650-8x24uq					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3277
catalyst_3850-24xs					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during	N/A	H-CIS-CATA-060820/3278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
catalyst_3850-48xs					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot	N/A	H-CIS-CATA-060820/3279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
catalyst_3850-nm-2-40g					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3280
catalyst_3850-nm-8-10g					
Improper Neutralization of Special Elements used in an OS	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local	N/A	H-CIS-CATA-060820/3281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
isr_4331					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ISR_-060820/3282
asr_1001-x					
Improper Privilege	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an	N/A	H-CIS-ASR_-060820/3283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
asr_1002-x					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-ASR_-060820/3284
asr_920-12sz-im					
Improper Input Validation	03-06-2020	6.8	A vulnerability in the Simple Network Management Protocol (SNMP) implementation in Cisco ASR 920 Series Aggregation Services Router model ASR920-12SZ-IM could allow an authenticated, remote attacker to cause the device to reload. The vulnerability is due to incorrect handling of data that is returned for Cisco	N/A	H-CIS-ASR_-060820/3285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Discovery Protocol queries to SNMP. An attacker could exploit this vulnerability by sending a request for Cisco Discovery Protocol information by using SNMP. An exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2020-3232**		
ucs_6248up					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-UCS_-060820/3286
ucs_6296up					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route	N/A	H-CIS-UCS_-060820/3287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
ucs_6332					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-UCS_-060820/3288
nexus_5010					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to	N/A	H-CIS-NEXU-060820/3289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3290
nexus_5020					
Improper Input	03-06-2020	8.3	A vulnerability in the Topology Discovery Service	N/A	H-CIS-NEXU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		060820/3291
Authenticati on Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated	N/A	H-CIS-NEXU-060820/3292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
ucs_6324					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-UCS_-060820/3293
ucs_6332-16up					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other	N/A	H-CIS-UCS_-060820/3294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected network behaviors. **CVE ID : CVE-2020-10136**		
catalyst_9800-40					
Uncontrolled Resource Consumption	03-06-2020	7.8	A vulnerability in the locally significant certificate (LSC) provisioning feature of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain public key infrastructure (PKI) packets. An attacker could exploit this vulnerability by sending crafted Secure Sockets Layer (SSL) packets to an affected device. A successful exploit could cause an affected device to continuously consume memory, which could result in a memory allocation failure that leads to a crash and causes a DoS condition. **CVE ID : CVE-2020-3203**	N/A	H-CIS-CATA-060820/3295
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied	N/A	H-CIS-CATA-060820/3296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
Improper Input Validation	03-06-2020	7.8	A vulnerability in the Flexible NetFlow Version 9 packet processor of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of parameters in a Flexible NetFlow Version 9 record. An attacker could exploit this vulnerability by sending a malformed Flexible NetFlow Version 9 packet to the Control and Provisioning of Wireless Access Points (CAPWAP) data port of an affected device. An exploit could allow the attacker to trigger an infinite loop, resulting in a process crash that would cause a reload of the device. **CVE ID : CVE-2020-3221**	N/A	H-CIS-CATA-060820/3297
catalyst_9800-80					
Uncontrolled Resource Consumption	03-06-2020	7.8	A vulnerability in the locally significant certificate (LSC) provisioning feature of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE	N/A	H-CIS-CATA-060820/3298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain public key infrastructure (PKI) packets. An attacker could exploit this vulnerability by sending crafted Secure Sockets Layer (SSL) packets to an affected device. A successful exploit could cause an affected device to continuously consume memory, which could result in a memory allocation failure that leads to a crash and causes a DoS condition. **CVE ID : CVE-2020-3203**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3299
Improper Input Validation	03-06-2020	7.8	A vulnerability in the Flexible NetFlow Version 9 packet processor of Cisco IOS XE Software for Cisco Catalyst 9800 Series	N/A	H-CIS-CATA-060820/3300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of parameters in a Flexible NetFlow Version 9 record. An attacker could exploit this vulnerability by sending a malformed Flexible NetFlow Version 9 packet to the Control and Provisioning of Wireless Access Points (CAPWAP) data port of an affected device. An exploit could allow the attacker to trigger an infinite loop, resulting in a process crash that would cause a reload of the device. **CVE ID : CVE-2020-3221**		
catalyst_9800-cl					
Uncontrolled Resource Consumption	03-06-2020	7.8	A vulnerability in the locally significant certificate (LSC) provisioning feature of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain public key infrastructure (PKI) packets. An attacker could	N/A	H-CIS-CATA-060820/3301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted Secure Sockets Layer (SSL) packets to an affected device. A successful exploit could cause an affected device to continuously consume memory, which could result in a memory allocation failure that leads to a crash and causes a DoS condition. **CVE ID : CVE-2020-3203**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3302
Improper Input Validation	03-06-2020	7.8	A vulnerability in the Flexible NetFlow Version 9 packet processor of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of parameters in a Flexible NetFlow Version 9 record. An attacker could exploit	N/A	H-CIS-CATA-060820/3303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a malformed Flexible NetFlow Version 9 packet to the Control and Provisioning of Wireless Access Points (CAPWAP) data port of an affected device. An exploit could allow the attacker to trigger an infinite loop, resulting in a process crash that would cause a reload of the device. **CVE ID : CVE-2020-3221**		
catalyst_9800-l					
Uncontrolled Resource Consumption	03-06-2020	7.8	A vulnerability in the locally significant certificate (LSC) provisioning feature of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain public key infrastructure (PKI) packets. An attacker could exploit this vulnerability by sending crafted Secure Sockets Layer (SSL) packets to an affected device. A successful exploit could cause an affected device to continuously consume memory, which could result in a memory allocation failure that leads to a crash	N/A	H-CIS-CATA-060820/3304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and causes a DoS condition. **CVE ID : CVE-2020-3203**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3305
Improper Input Validation	03-06-2020	7.8	A vulnerability in the Flexible NetFlow Version 9 packet processor of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of parameters in a Flexible NetFlow Version 9 record. An attacker could exploit this vulnerability by sending a malformed Flexible NetFlow Version 9 packet to the Control and Provisioning of Wireless Access Points (CAPWAP) data port of an affected device. An exploit could allow the attacker to trigger an infinite loop, resulting in a process crash	N/A	H-CIS-CATA-060820/3306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that would cause a reload of the device. **CVE ID : CVE-2020-3221**		
catalyst_9800-l-c					
Uncontrolled Resource Consumption	03-06-2020	7.8	A vulnerability in the locally significant certificate (LSC) provisioning feature of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain public key infrastructure (PKI) packets. An attacker could exploit this vulnerability by sending crafted Secure Sockets Layer (SSL) packets to an affected device. A successful exploit could cause an affected device to continuously consume memory, which could result in a memory allocation failure that leads to a crash and causes a DoS condition. **CVE ID : CVE-2020-3203**	N/A	H-CIS-CATA-060820/3307
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied	N/A	H-CIS-CATA-060820/3308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
Improper Input Validation	03-06-2020	7.8	A vulnerability in the Flexible NetFlow Version 9 packet processor of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of parameters in a Flexible NetFlow Version 9 record. An attacker could exploit this vulnerability by sending a malformed Flexible NetFlow Version 9 packet to the Control and Provisioning of Wireless Access Points (CAPWAP) data port of an affected device. An exploit could allow the attacker to trigger an infinite loop, resulting in a process crash that would cause a reload of the device. **CVE ID : CVE-2020-3221**	N/A	H-CIS-CATA-060820/3309
catalyst_9800-l-f					
Uncontrolled Resource Consumption	03-06-2020	7.8	A vulnerability in the locally significant certificate (LSC) provisioning feature of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE	N/A	H-CIS-CATA-060820/3310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain public key infrastructure (PKI) packets. An attacker could exploit this vulnerability by sending crafted Secure Sockets Layer (SSL) packets to an affected device. A successful exploit could cause an affected device to continuously consume memory, which could result in a memory allocation failure that leads to a crash and causes a DoS condition. **CVE ID : CVE-2020-3203**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3311
Improper Input Validation	03-06-2020	7.8	A vulnerability in the Flexible NetFlow Version 9 packet processor of Cisco IOS XE Software for Cisco Catalyst 9800 Series	N/A	H-CIS-CATA-060820/3312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of parameters in a Flexible NetFlow Version 9 record. An attacker could exploit this vulnerability by sending a malformed Flexible NetFlow Version 9 packet to the Control and Provisioning of Wireless Access Points (CAPWAP) data port of an affected device. An exploit could allow the attacker to trigger an infinite loop, resulting in a process crash that would cause a reload of the device. **CVE ID : CVE-2020-3221**		
catalyst_c9200-24p					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this	N/A	H-CIS-CATA-060820/3313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3314
catalyst_c9200-24t					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker	N/A	H-CIS-CATA-060820/3315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3316
catalyst_c9200-48p					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing	N/A	H-CIS-CATA-060820/3317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3318
catalyst_c9200-48t					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation	N/A	H-CIS-CATA-060820/3319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3320
catalyst_c9200l-24p-4g					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to	N/A	H-CIS-CATA-060820/3321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3322
catalyst_c9200l-24p-4x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This	N/A	H-CIS-CATA-060820/3323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3324
catalyst_c9200l-24pxg-2y					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during	N/A	H-CIS-CATA-060820/3325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3326
catalyst_c9200l-24pxg-4x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command	N/A	H-CIS-CATA-060820/3327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3328
catalyst_c9200l-24t-4g					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to	N/A	H-CIS-CATA-060820/3329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3330
catalyst_c9200l-24t-4x					
Improper Neutralization of Special Elements used in an OS Command ('OS	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying	N/A	H-CIS-CATA-060820/3331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3332
ws-c3850-12x48u					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability	N/A	H-CIS-WS-C-060820/3333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
ws-c3850-12xs					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3334
ws-c3850-24p					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3335
ws-c3850-24s					
Improper Privilege	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an	N/A	H-CIS-WS-C-060820/3336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
ws-c3850-24t					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3337
ws-c3850-24u					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ws-c3850-24xs					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3339
ws-c3850-24xu					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3340
ws-c3850-48f					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to	N/A	H-CIS-WS-C-060820/3341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
ws-c3850-48p					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3342
ws-c3850-48t					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3343
ws-c3850-48u					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability	N/A	H-CIS-WS-C-060820/3344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
ws-c3850-48xs					
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-WS-C-060820/3345
nexus_3016q					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service	N/A	H-CIS-NEXU-060820/3346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
nexus_3064t					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a	N/A	H-CIS-NEXU-060820/3347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
nexus_3064x					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to	N/A	H-CIS-NEXU-060820/3348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
nexus_5000					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative	N/A	H-CIS-NEXU-060820/3349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
catalyst_4503-e					
Improper Input Validation	03-06-2020	6.3	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software on Catalyst 4500 Series Switches could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient input validation when the software processes specific SNMP object identifiers. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: To exploit this vulnerability by using SNMPv2c or earlier, the attacker must know the SNMP read-only community string for an affected system. To exploit this vulnerability by using SNMPv3, the attacker must know the user credentials for the affected system.	N/A	H-CIS-CATA-060820/3350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3235		
catalyst_4506-e					
Improper Input Validation	03-06-2020	6.3	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software on Catalyst 4500 Series Switches could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient input validation when the software processes specific SNMP object identifiers. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: To exploit this vulnerability by using SNMPv2c or earlier, the attacker must know the SNMP read-only community string for an affected system. To exploit this vulnerability by using SNMPv3, the attacker must know the user credentials for the affected system. **CVE ID : CVE-2020-3235**	N/A	H-CIS-CATA-060820/3351
catalyst_4507r\+e					
Improper Input	03-06-2020	6.3	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem	N/A	H-CIS-CATA-060820/3352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			of Cisco IOS Software and Cisco IOS XE Software on Catalyst 4500 Series Switches could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient input validation when the software processes specific SNMP object identifiers. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: To exploit this vulnerability by using SNMPv2c or earlier, the attacker must know the SNMP read-only community string for an affected system. To exploit this vulnerability by using SNMPv3, the attacker must know the user credentials for the affected system. **CVE ID : CVE-2020-3235**		
catalyst_4510r\+e					
Improper Input Validation	03-06-2020	6.3	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software on Catalyst 4500 Series Switches could allow an authenticated, remote	N/A	H-CIS-CATA-060820/3353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient input validation when the software processes specific SNMP object identifiers. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: To exploit this vulnerability by using SNMPv2c or earlier, the attacker must know the SNMP read-only community string for an affected system. To exploit this vulnerability by using SNMPv3, the attacker must know the user credentials for the affected system. **CVE ID : CVE-2020-3235**		
ir809g-lte-ga-k9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR80-060820/3354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR80-060820/3355
ir809g-lte-la-k9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR80-060820/3356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR80-060820/3357
ir809g-lte-na-k9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR80-060820/3358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR80-060820/3359
ir809g-lte-vz-k9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR80-060820/3360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR80-060820/3361
ir829-2lte-ea-ak9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR82-060820/3362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR82-060820/3363
ir829-2lte-ea-bk9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR82-060820/3364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR82-060820/3365
ir829-2lte-ea-ek9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR82-060820/3366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR82-060820/3367
ir829gw-lte-ga-ck9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR82-060820/3368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR82-060820/3369
ir829gw-lte-ga-ek9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR82-060820/3370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR82-060820/3371
ir829gw-lte-ga-sk9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR82-060820/3372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR82-060820/3373
ir829gw-lte-ga-zk9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR82-060820/3374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR82-060820/3375
ir829gw-lte-na-ak9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR82-060820/3376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR82-060820/3377
ir829gw-lte-vz-ak9					
Improper Input Validation	03-06-2020	4.8	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated	N/A	H-CIS-IR82-060820/3378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3257**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2020	10	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3258**	N/A	H-CIS-IR82-060820/3379
catalyst_c9200l-48p-4g					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation	N/A	H-CIS-CATA-060820/3380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3381
catalyst_c9200l-48p-4x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to	N/A	H-CIS-CATA-060820/3382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3383
catalyst_c9200l-48pxg-2y					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This	N/A	H-CIS-CATA-060820/3384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3385
catalyst_c9200l-48pxg-4x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during	N/A	H-CIS-CATA-060820/3386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3387
catalyst_c9200l-48t-4g					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command	N/A	H-CIS-CATA-060820/3388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3389
catalyst_c9200l-48t-4x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to	N/A	H-CIS-CATA-060820/3390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3391
catalyst_c9300-24p					
Improper Neutralization of Special Elements used in an OS Command ('OS	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying	N/A	H-CIS-CATA-060820/3392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3393
catalyst_c9300-24s					
Improper Neutralization of Special Elements used in an OS Command	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell	N/A	H-CIS-CATA-060820/3394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3395
catalyst_c9300-24t					
Improper Neutralization of Special Elements used in an OS	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local	N/A	H-CIS-CATA-060820/3396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3397
catalyst_c9300-24u					
Improper Neutralization of Special Elements	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could	N/A	H-CIS-CATA-060820/3398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3399
catalyst_c9300-24ux					
Improper Neutralization of Special	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE	N/A	H-CIS-CATA-060820/3400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3401
catalyst_c9300-48p					
Improper Neutralizatio	03-06-2020	7.2	A vulnerability in the processing of boot options of	N/A	H-CIS-CATA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		060820/3402
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3403
catalyst_c9300-48s					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3404
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
catalyst_c9300-48t					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3406
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device.	N/A	H-CIS-CATA-060820/3407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3214		
catalyst_c9300-48u					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3408
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto	N/A	H-CIS-CATA-060820/3409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. **CVE ID : CVE-2020-3214**		
catalyst_c9300-48un					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3410
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to	N/A	H-CIS-CATA-060820/3411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
catalyst_c9300-48uxm					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3412
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability	N/A	H-CIS-CATA-060820/3413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
catalyst_c9300l-24p-4g					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3414
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied	N/A	H-CIS-CATA-060820/3415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
catalyst_c9300l-24p-4x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3416
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient	N/A	H-CIS-CATA-060820/3417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
catalyst_c9300l-24t-4g					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3418
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability	N/A	H-CIS-CATA-060820/3419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
catalyst_c9300l-24t-4x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3420
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level	N/A	H-CIS-CATA-060820/3421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
catalyst_c9300l-48p-4g					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3422
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to	N/A	H-CIS-CATA-060820/3423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
catalyst_c9300l-48p-4x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3424
Improper Privilege	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker	N/A	H-CIS-CATA-060820/3425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		
catalyst_c9300l-48t-4g					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3426
Improper Privilege	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an	N/A	H-CIS-CATA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**		060820/3427
catalyst_c9300l-48t-4x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**	N/A	H-CIS-CATA-060820/3428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3429
catalyst_c9500-12q					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges.	N/A	H-CIS-CATA-060820/3430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3207		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3431
catalyst_c9500-16x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-	N/A	H-CIS-CATA-060820/3432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3433
catalyst_c9500-24q					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an	N/A	H-CIS-CATA-060820/3434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3435
catalyst_c9500-24y4c					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute	N/A	H-CIS-CATA-060820/3436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3437
catalyst_c9500-32c					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot	N/A	H-CIS-CATA-060820/3438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3439
catalyst_c9500-32qc					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to	N/A	H-CIS-CATA-060820/3440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3441
catalyst_c9500-40x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit	N/A	H-CIS-CATA-060820/3442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3443
catalyst_c9500-48y4c					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.2	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided	N/A	H-CIS-CATA-060820/3444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges. **CVE ID : CVE-2020-3207**		
Improper Privilege Management	03-06-2020	7.2	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device. **CVE ID : CVE-2020-3214**	N/A	H-CIS-CATA-060820/3445
nexus_1000ve					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3446
nexus_92304qc					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3447
nexus_92348gc-x					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3448
nexus_9236c					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-	N/A	H-CIS-NEXU-060820/3449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_9272q					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3450
nexus_93108tc-ex					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an	N/A	H-CIS-NEXU-060820/3451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_93108tc-fx					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3452
nexus_93120tx					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors.	N/A	H-CIS-NEXU-060820/3453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10136		
nexus_93128tx					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3454
nexus_93180lc-ex					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3455
nexus_93180yc-ex					
Authentication Bypass by	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP	N/A	H-CIS-NEXU-060820/3456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Spoofing			standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_93180yc-fx					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3457
nexus_93216tc-fx2					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated	N/A	H-CIS-NEXU-060820/3458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_93240yc-fx2					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3459
nexus_9332c					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other	N/A	H-CIS-NEXU-060820/3460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_9332pq					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3461
nexus_93360yc-fx2					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3462
nexus_9336c-fx2					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3463
nexus_9336pq_aci_spine					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3464
nexus_9348gc-fxp					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-	N/A	H-CIS-NEXU-060820/3465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_9364c					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3466
nexus_9372px					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an	N/A	H-CIS-NEXU-060820/3467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_9372px-e					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3468
nexus_9372tx					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors.	N/A	H-CIS-NEXU-060820/3469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10136		
nexus_9372tx-e					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3470
nexus_9396px					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3471
nexus_9396tx					
Authentication Bypass by	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP	N/A	H-CIS-NEXU-060820/3472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Spoofing			standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_9504					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3473
nexus_9508					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated	N/A	H-CIS-NEXU-060820/3474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_9516					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3475
nexus_3016					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The	N/A	H-CIS-NEXU-060820/3476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3477
nexus_3048					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**	N/A	H-CIS-NEXU-060820/3478
Authenticati on Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any	N/A	H-CIS-NEXU-060820/3479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**		
nexus_3064					
Improper Input Validation	03-06-2020	8.3	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative	N/A	H-CIS-NEXU-060820/3480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition. **CVE ID : CVE-2020-3217**		
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3481
nexus_3064-t					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-CIS-NEXU-060820/3482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wap131					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-CIS-WAP1-060820/3483
wap150					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-CIS-WAP1-060820/3484
wap351					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue.	N/A	H-CIS-WAP3-060820/3485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12695		
Dell					
g3_15_3590					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-G3_1-060820/3486
g5_15_5590					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-G5_1-060820/3487
g5_5090					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-G5_5-060820/3488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
g7_15_7590					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-G7_1-060820/3489
g7_17_7790					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-G7_1-060820/3490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_14_5490					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3491
inspiron_3490					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3492
inspiron_3493					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3493
inspiron_3590					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3494
inspiron_3593					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	H-DEL-INSP-060820/3495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_3790					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3496
inspiron_3793					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	H-DEL-INSP-060820/3497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
inspiron_5390					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3498
inspiron_5391					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3499
inspiron_5493					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	H-DEL-INSP-060820/3500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5494					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3501
inspiron_5498					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	H-DEL-INSP-060820/3502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5583					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3503
inspiron_5584					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3504
inspiron_5590					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	H-DEL-INSP-060820/3505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5593					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3506
inspiron_5594					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	H-DEL-INSP-060820/3507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5598					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3508
inspiron_7391					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
inspiron_7490					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3510
inspiron_7590					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3511
inspiron_7591					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	H-DEL-INSP-060820/3512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3301					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3513
latitude_3300					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	H-DEL-LATI-060820/3514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
latitude_3400					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3515
latitude_3500					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3516
latitude_5300					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows	N/A	H-DEL-LATI-060820/3517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**		
latitude_5400					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	H-DEL-LATI-060820/3518
latitude_5401					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface	N/A	H-DEL-LATI-060820/3519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**		
latitude_5420_rugged					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3520
latitude_5424_rugged					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator	N/A	H-DEL-LATI-060820/3521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5500					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	H-DEL-LATI-060820/3522
latitude_5501					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive.	N/A	H-DEL-LATI-060820/3523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5363		
latitude_7220ex_rugged_extreme_tablet					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	H-DEL-LATI-060820/3524
latitude_7300					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	H-DEL-LATI-060820/3525
latitude_7400					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	H-DEL-LATI-060820/3526
precision_3540					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	H-DEL-PREC-060820/3527
precision_3541					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-PREC-060820/3528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	H-DEL-PREC-060820/3529
precision_5540					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-PREC-060820/3530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_7540					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	H-DEL-PREC-060820/3531
precision_7730					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
precision_7740					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	H-DEL-PREC-060820/3533
vostro_15_7580					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3534
vostro_3481					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability	N/A	H-DEL-VOST-060820/3535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3490					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3536
vostro_3590					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator	N/A	H-DEL-VOST-060820/3537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_5390					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3538
vostro_5391					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3539
vostro_5490					
Missing	10-06-2020	2.1	Dell Client Consumer and	N/A	H-DEL-VOST-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		060820/3540
vostro_5590					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3541
vostro_7590					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS	N/A	H-DEL-VOST-060820/3542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
wyse_5070_thin_client					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-WYSE-060820/3543
wyse_5470					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-WYSE-060820/3544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xps_13_9380					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-XPS_-060820/3545
xps_15_9570					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-XPS_-060820/3546
inspiron_14_gaming_7466					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	H-DEL-INSP-060820/3547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_14_gaming_7467					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3548
inspiron_15_7572					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	H-DEL-INSP-060820/3549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
inspiron_15_gaming_7566					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3550
inspiron_15_gaming_7567					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3551
chengming_3967					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-CHEN-060820/3552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
g3_3779					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-G3_3-060820/3553
latitude_3460					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-LATI-060820/3554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3470					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3555
latitude_3480					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3556
latitude_3490					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3557
latitude_3560					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3558
latitude_3570					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	H-DEL-LATI-060820/3559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3580					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3560
latitude_3590					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	H-DEL-LATI-060820/3561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
latitude_5175					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3562
latitude_5179					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3563
latitude_5250					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	H-DEL-LATI-060820/3564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5280					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3565
latitude_5285					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	H-DEL-LATI-060820/3566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5288					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3567
latitude_5289					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3568
latitude_5290					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	H-DEL-LATI-060820/3569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5290_2-in-1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3570
latitude_5450					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	H-DEL-LATI-060820/3571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5480					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3572
latitude_5488					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
latitude_5490					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3574
latitude_5491					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3575
latitude_5550					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	H-DEL-LATI-060820/3576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_5510					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3577
precision_5520					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	H-DEL-PREC-060820/3578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
precision_5530					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3579
precision_5720_aio					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3580
precision_7510					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-PREC-060820/3581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_7520					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3582
precision_7530					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-PREC-060820/3583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_7710					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3584
precision_7720					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3585
precision_7820					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3586
precision_7920					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3587
vostro_3070					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	H-DEL-VOST-060820/3588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3267					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3589
chengming_3977					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	H-DEL-CHEN-060820/3590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
chengming_3980					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-CHEN-060820/3591
xps_8900					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-XPS_-060820/3592
g3_3579					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	H-DEL-G3_3-060820/3593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
g5_5587					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-G5_5-060820/3594
g7_7588					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	H-DEL-G7_7-060820/3595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
embedded_box_pc_5000					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-EMBE-060820/3596
latitude_5580					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3597
latitude_5590					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	H-DEL-LATI-060820/3598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5591					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3599
latitude_7250					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	H-DEL-LATI-060820/3600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_7275					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3601
latitude_7280					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
latitude_7285					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3603
latitude_7290					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3604
latitude_7350					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	H-DEL-LATI-060820/3605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_7370					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3606
latitude_7380					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	H-DEL-LATI-060820/3607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
latitude_7389					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3608
latitude_7390					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3609
latitude_7390_2-in-1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-LATI-060820/3610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_7424_rugged_extreme					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3611
latitude_7480					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-LATI-060820/3612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_7490					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3613
latitude_e5250					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3614
latitude_e5270					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3615
latitude_e5450					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3616
latitude_e5470					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	H-DEL-LATI-060820/3617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_e5550					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3618
latitude_e5570					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	H-DEL-LATI-060820/3619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
latitude_e7250					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3620
latitude_e7270					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3621
latitude_e7450					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	H-DEL-LATI-060820/3622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_e7470					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3623
optiplex_3040					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	H-DEL-OPTI-060820/3624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_3046					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3625
optiplex_3050					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3626
optiplex_3050_aio					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	H-DEL-OPTI-060820/3627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_3060					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3628
optiplex_3240_aio					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	H-DEL-OPTI-060820/3629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_5040					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3630
optiplex_5060					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
optiplex_5260_aio					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3632
optiplex_7050					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3633
optiplex_7060					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	H-DEL-OPTI-060820/3634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_7440_aio					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3635
optiplex_7460_aio					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	H-DEL-OPTI-060820/3636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
optiplex_7760_aio					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3637
optiplex_xe3					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3638
precision_3430					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-PREC-060820/3639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_3510					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3640
precision_3520					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-PREC-060820/3641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_3530					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3642
precision_3930_rack					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3643
precision_5530_2-in_1					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3644
precision_5550					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3645
precision_5820_tower					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	H-DEL-PREC-060820/3646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_7820_tower					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3647
precision_7920_tower					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	H-DEL-PREC-060820/3648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
precision_tower_3431_small_form_factor					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3649
vostro_14_3468					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3650
vostro_14_3478					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	H-DEL-VOST-060820/3651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_14_5468					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3652
vostro_15_3568					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	H-DEL-VOST-060820/3653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_15_3578					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3654
vostro_15_5568					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3655
vostro_3471					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	H-DEL-VOST-060820/3656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3491					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3657
vostro_3558					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	H-DEL-VOST-060820/3658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3559					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3659
vostro_3591					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vostro_3671					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3661
vostro_3681					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3662
vostro_3881					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	H-DEL-VOST-060820/3663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3888					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3664
vostro_5090					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	H-DEL-VOST-060820/3665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
vostro_5300					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3666
vostro_5880					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3667
vostro_7500					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-VOST-060820/3668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
wyse_5470_all-in-one					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-WYSE-060820/3669
wyse_7040_thin_client					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-WYSE-060820/3670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_15_gaming_7577					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3671
inspiron_3670					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3672
optiplex_3070					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3673
optiplex_5070					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3674
optiplex_5250					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	H-DEL-OPTI-060820/3675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_7070					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3676
vostro_15_7570					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	H-DEL-VOST-060820/3677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
xps_12_9250					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-XPS_-060820/3678
xps_13_9360					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-XPS_-060820/3679
xps_15_9560					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	H-DEL-XPS_-060820/3680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
chengming_3988					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-CHEN-060820/3681
chengming_3990					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	H-DEL-CHEN-060820/3682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
chengming_3991					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-CHEN-060820/3683
g3_15_3500					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-G3_1-060820/3684
g5_15_5500					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	H-DEL-G5_1-060820/3685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_11_2-in-1_3153					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3686
inspiron_11_2-in-1_3158					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	H-DEL-INSP-060820/3687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_13_7370					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3688
inspiron_13_2-in-1_5368					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
inspiron_13_2-in-1_5378					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3690
inspiron_13_2-in-1_5379					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3691
inspiron_13_2-in-1_7353					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	H-DEL-INSP-060820/3692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_13_2-in-1_7359					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3693
inspiron_13_2-in-1_7368					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	H-DEL-INSP-060820/3694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
inspiron_13_2-in-1_7373					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3695
inspiron_13_2-in-1_7378					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3696
inspiron_14_3458					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-INSP-060820/3697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_14_3459					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3698
inspiron_14_3467					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-INSP-060820/3699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_14_3468					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3700
inspiron_14_3473					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3701
inspiron_14_5468					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3702
inspiron_14_7460					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3703
inspiron_15_3559					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	H-DEL-INSP-060820/3704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
xps_13_9370					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-XPS_-060820/3705
xps_13_2-in-1_9365					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	H-DEL-XPS_-060820/3706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
xps_13_9300					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-XPS_-060820/3707
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	H-DEL-XPS_-060820/3708
xps_15_2-in-1_9575					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability	N/A	H-DEL-XPS_-060820/3709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
xps_15_7500					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-XPS_-060820/3710
xps_27_aio_7760					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator	N/A	H-DEL-XPS_-060820/3711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
xps_7380					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-XPS_-060820/3712
xps_7390_2-in-1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-XPS_-060820/3713
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows	N/A	H-DEL-XPS_-060820/3714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**		
latitude_7200_2_in_1					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	H-DEL-LATI-060820/3715
latitude_7220					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface	N/A	H-DEL-LATI-060820/3716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**		
xps_7590					
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**	N/A	H-DEL-XPS_-060820/3717
inspiron_3268					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	H-DEL-INSP-060820/3718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_3470					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3719
inspiron_3476					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
inspiron_3480					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3721
inspiron_3481					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3722
inspiron_3576					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	H-DEL-INSP-060820/3723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_3580					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3724
inspiron_3583					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	H-DEL-INSP-060820/3725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
inspiron_3581					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3726
inspiron_3584					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3727
inspiron_3668					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-INSP-060820/3728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_3780					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3729
inspiron_3781					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-INSP-060820/3730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5370					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3731
inspiron_5457					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3732
inspiron_15_3567					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3733
inspiron_15_3568					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3734
inspiron_15_5566					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	H-DEL-INSP-060820/3735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_15_5567					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3736
inspiron_15_7560					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	H-DEL-INSP-060820/3737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
inspiron_15_7570					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3738
inspiron_15_2-in-1_5568					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3739
inspiron_15_2-in-1_5578					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	H-DEL-INSP-060820/3740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_15_2-in-1_5579					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3741
inspiron_15_2-in-1_7568					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	H-DEL-INSP-060820/3742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_15_2-in-1_7569					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3743
inspiron_15_2-in-1_7573					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3744
inspiron_15_2-in-1_7579					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	H-DEL-INSP-060820/3745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_15-3552					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3746
inspiron_17_5767					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	H-DEL-INSP-060820/3747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_17_2-in-1_7773					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3748
inspiron_17_2-in-1_7778					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
inspiron_17_2-in-1_7779					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3750
inspiron_3471					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3751
inspiron_3671					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	H-DEL-INSP-060820/3752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_3880					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3753
inspiron_3881					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	H-DEL-INSP-060820/3754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
inspiron_5300					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3755
inspiron_5400_2_in1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3756
inspiron_5491_2_in_1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-INSP-060820/3757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5591_2-in-1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3758
inspiron_5459					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-INSP-060820/3759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5480					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3760
inspiron_5481					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3761
inspiron_5482					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3762
inspiron_5557					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3763
inspiron_5559					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	H-DEL-INSP-060820/3764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_5570					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3765
inspiron_5580					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	H-DEL-INSP-060820/3766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
inspiron_5582					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3767
inspiron_5759					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3768
inspiron_5770					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	H-DEL-INSP-060820/3769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_7380					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3770
inspiron_7386					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	H-DEL-INSP-060820/3771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_7472					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3772
inspiron_7580					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3773
inspiron_7586					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	H-DEL-INSP-060820/3774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_7786					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3775
latitude_3180					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	H-DEL-LATI-060820/3776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3189					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3777
latitude_3190					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
latitude_3350					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3779
latitude_3379					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3780
latitude_3380					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	H-DEL-LATI-060820/3781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_7300_2_in_1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3782
inspiron_7390_2_in_1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	H-DEL-INSP-060820/3783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
inspiron_7391_2_in_1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3784
inspiron_7500					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3785
inspiron_7500_2_in_1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-INSP-060820/3786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_7501					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3787
inspiron_7590_2_in_1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-INSP-060820/3788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
inspiron_7591_2_in_1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3789
inspiron_5490_aio					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3790
inspiron_7790_aio					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3791
insprion_5491_aio					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-INSP-060820/3792
latitude_3190_2-in-1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	H-DEL-LATI-060820/3793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3310					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3794
latitude_3310_2-in-1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	H-DEL-LATI-060820/3795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
latitude_3390_2-in-1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3796
latitude_3410					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3797
latitude_3460_mobile_thin_client					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	H-DEL-LATI-060820/3798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_3480_mobile_thin_client					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3799
latitude_3510					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	H-DEL-LATI-060820/3800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5280_mobile_thin_client					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3801
latitude_5300_2-in-1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3802
N/A	10-06-2020	7.2	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to	N/A	H-DEL-LATI-060820/3803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive. **CVE ID : CVE-2020-5363**		
latitude_5310					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3804
latitude_5310_2_in_1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	H-DEL-LATI-060820/3805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_5410					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3806
latitude_5411					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
latitude_5414_rugged					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3808
latitude_5510					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3809
latitude_5511					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	H-DEL-LATI-060820/3810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_7210_2_in_1					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3811
latitude_7212_rugged_extreme_tablet					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	H-DEL-LATI-060820/3812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
latitude_7214_rugged_extreme					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3813
latitude_7310					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3814
latitude_7410					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-LATI-060820/3815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_7414_rugged					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3816
latitude_9410					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-LATI-060820/3817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
latitude_9510					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3818
latitude_e7270_mobile_thin_client					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-LATI-060820/3819
optiplex_3280_aio					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3820
optiplex_5080					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3821
optiplex_5270_aio					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	H-DEL-OPTI-060820/3822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_5480_aio					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3823
optiplex_7071_tower					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	H-DEL-OPTI-060820/3824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
optiplex_7080					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3825
optiplex_7480_aio					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3826
optiplex_7780_aio					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	H-DEL-OPTI-060820/3827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
optiplex_aio_7470					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3828
optiplex_aio_7770					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore	N/A	H-DEL-OPTI-060820/3829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_3420_tower					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3830
precision_3440					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3831
precision_3550					
Missing Authorizatio	10-06-2020	2.1	Dell Client Consumer and Commercial platforms	N/A	H-DEL-PREC-060820/3832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_3551					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3833
precision_3620_tower					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges,	N/A	H-DEL-PREC-060820/3834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
precision_3630_tower					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3835
precision_3640_tower					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-PREC-060820/3836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
optiplex_7450					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3837
optiplex_7040					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-OPTI-060820/3838
optiplex_5050					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an	N/A	H-DEL-OPTI-060820/3839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3268					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3840
vostro_3458					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to	N/A	H-DEL-VOST-060820/3841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default values. **CVE ID : CVE-2020-5362**		
vostro_3459					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3842
vostro_3470					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3843
vostro_3480					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper	N/A	H-DEL-VOST-060820/3844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3580					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3845
vostro_3581					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS	N/A	H-DEL-VOST-060820/3846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3584					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3847
vostro_3583					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3848
vostro_3660					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3849
vostro_3667					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3850
vostro_3668					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with	N/A	H-DEL-VOST-060820/3851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_3669					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3852
vostro_3670					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	N/A	H-DEL-VOST-060820/3853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5362		
vostro_5370					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3854
vostro_5471					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3855
vostro_5481					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability	N/A	H-DEL-VOST-060820/3856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**		
vostro_5581					
Missing Authorization	10-06-2020	2.1	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values. **CVE ID : CVE-2020-5362**	N/A	H-DEL-VOST-060820/3857
b1165nfw					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-DEL-B116-060820/3858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dlink					
dsl-2730u					
N/A	08-06-2020	5	D-Link DSL 2730-U IN_1.10 and IN_1.11 and DIR-600M 3.04 devices have the domain.name string in the DNS resolver search path by default, which allows remote attackers to provide valid DNS responses (and also offer Internet services such as HTTP) for names that otherwise would have had an NXDOMAIN error, by registering a subdomain of the domain.name domain name. **CVE ID : CVE-2020-13960**	N/A	H-DLI-DSL--060820/3859
dir-865l					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-06-2020	7.5	D-Link DIR-865L Ax 1.20B01 Beta devices allow Command Injection. **CVE ID : CVE-2020-13782**	N/A	H-DLI-DIR--060820/3860
Information Exposure	03-06-2020	5	D-Link DIR-865L Ax 1.20B01 Beta devices have Cleartext Storage of Sensitive Information. **CVE ID : CVE-2020-13783**	N/A	H-DLI-DIR--060820/3861
Use of Cryptographically Weak Pseudo-Random Number	03-06-2020	5	D-Link DIR-865L Ax 1.20B01 Beta devices have a predictable seed in a Pseudo-Random Number Generator.	N/A	H-DLI-DIR--060820/3862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generator (PRNG)			**CVE ID : CVE-2020-13784**		
Inadequate Encryption Strength	03-06-2020	5	D-Link DIR-865L Ax 1.20B01 Beta devices have Inadequate Encryption Strength. **CVE ID : CVE-2020-13785**	N/A	H-DLI-DIR--060820/3863
Cross-Site Request Forgery (CSRF)	03-06-2020	6.8	D-Link DIR-865L Ax 1.20B01 Beta devices allow CSRF. **CVE ID : CVE-2020-13786**	N/A	H-DLI-DIR--060820/3864
Information Exposure	03-06-2020	5	D-Link DIR-865L Ax 1.20B01 Beta devices have Cleartext Transmission of Sensitive Information. **CVE ID : CVE-2020-13787**	N/A	H-DLI-DIR--060820/3865
dsl-2750u					
Missing Authentication for Critical Function	15-06-2020	4.6	D-link DSL-2750U ISL2750UEME3.V1E devices allow approximately 90 seconds of access to the control panel, after a restart, before MAC address filtering rules become active. **CVE ID : CVE-2020-13150**	N/A	H-DLI-DSL--060820/3866
dir-600m					
N/A	08-06-2020	5	D-Link DSL 2730-U IN_1.10 and IN_1.11 and DIR-600M 3.04 devices have the domain.name string in the DNS resolver search path by default, which allows remote attackers to provide valid DNS responses (and also offer Internet services such as HTTP) for names that otherwise would have had an NXDOMAIN error, by	N/A	H-DLI-DIR--060820/3867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			registering a subdomain of the domain.name domain name. **CVE ID : CVE-2020-13960**		
D-link					
dvg-n5412sp					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-D-L-DVG--060820/3868
Epson					
xp-970					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-9-060820/3869
xp-960					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription	N/A	H-EPS-XP-9-060820/3870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
xp-8500					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-8-060820/3871
xp-8600					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-8-060820/3872
ep-101					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the	N/A	H-EPS-EP-1-060820/3873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
ew-m970a3t					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-EW-M-060820/3874
m571t					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-M571-060820/3875
xp-100					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-	N/A	H-EPS-XP-1-060820/3876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
xp-2101					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-2-060820/3877
xp-2105					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-2-060820/3878
xp-241					
Incorrect Default	08-06-2020	7.8	The Open Connectivity Foundation UPnP	N/A	H-EPS-XP-2-060820/3879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
xp-320					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-3-060820/3880
xp-330					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-3-060820/3881
xp-340					
Incorrect	08-06-2020	7.8	The Open Connectivity	N/A	H-EPS-XP-3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Default Permissions			Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		060820/3882
xp-4100					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-4-060820/3883
xp-4105					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-4-060820/3884
xp-440					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-4-060820/3885
xp-620					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-6-060820/3886
xp-630					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-6-060820/3887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xp-702					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-EPS-XP-7-060820/3888
GE					
rt430					
Missing Authenticati on for Critical Function	02-06-2020	9	GE Grid Solutions Reason RT Clocks, RT430, RT431, and RT434, all firmware versions prior to 08A05. The device's vulnerability in the web application could allow multiple unauthenticated attacks that could cause serious impact. The vulnerability may allow an unauthenticated attacker to execute arbitrary commands and send a request to a specific URL that could cause the device to become unresponsive. The unauthenticated attacker may change the password of the 'configuration' user account, allowing the attacker to modify the configuration of the device via the web interface using the new password. This vulnerability may also allow	N/A	H-GE-RT43-060820/3889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated attacker to bypass the authentication required to configure the device and reboot the system. **CVE ID : CVE-2020-12017**		
rt431					
Missing Authenticati on for Critical Function	02-06-2020	9	GE Grid Solutions Reason RT Clocks, RT430, RT431, and RT434, all firmware versions prior to 08A05. The device's vulnerability in the web application could allow multiple unauthenticated attacks that could cause serious impact. The vulnerability may allow an unauthenticated attacker to execute arbitrary commands and send a request to a specific URL that could cause the device to become unresponsive. The unauthenticated attacker may change the password of the 'configuration' user account, allowing the attacker to modify the configuration of the device via the web interface using the new password. This vulnerability may also allow an unauthenticated attacker to bypass the authentication required to configure the device and reboot the system. **CVE ID : CVE-2020-12017**	N/A	H-GE-RT43-060820/3890
rt434					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	02-06-2020	9	GE Grid Solutions Reason RT Clocks, RT430, RT431, and RT434, all firmware versions prior to 08A05. The device's vulnerability in the web application could allow multiple unauthenticated attacks that could cause serious impact. The vulnerability may allow an unauthenticated attacker to execute arbitrary commands and send a request to a specific URL that could cause the device to become unresponsive. The unauthenticated attacker may change the password of the 'configuration' user account, allowing the attacker to modify the configuration of the device via the web interface using the new password. This vulnerability may also allow an unauthenticated attacker to bypass the authentication required to configure the device and reboot the system. **CVE ID : CVE-2020-12017**	N/A	H-GE-RT43-060820/3891
homey					
homey					
Cleartext Storage of Sensitive Information	04-06-2020	3.3	An issue was discovered in all Athom Homey and Homey Pro devices up to the current version 4.2.0. An attacker within RF range can obtain a cleartext copy of the network configuration of the	N/A	H-HOM-HOME-060820/3892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device, including the Wi-Fi PSK, during device setup. Upon success, the attacker is able to further infiltrate the target's Wi-Fi networks. **CVE ID : CVE-2020-9462**		
homey_pro					
Cleartext Storage of Sensitive Information	04-06-2020	3.3	An issue was discovered in all Athom Homey and Homey Pro devices up to the current version 4.2.0. An attacker within RF range can obtain a cleartext copy of the network configuration of the device, including the Wi-Fi PSK, during device setup. Upon success, the attacker is able to further infiltrate the target's Wi-Fi networks. **CVE ID : CVE-2020-9462**	N/A	H-HOM-HOME-060820/3893
HP					
x3220nr_firmware					
Authentication Bypass by Spoofing	02-06-2020	5	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors. **CVE ID : CVE-2020-10136**	N/A	H-HP-X322-060820/3894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
envy_4512_k9h49a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3895
envy_4513_k9h51a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3896
envy_4516_k9h52a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue.	N/A	H-HP-ENVY-060820/3897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12695		
envy_4520_e6g67a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3898
envy_4520_e6g67b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3899
envy_4520_f0v63a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger	N/A	H-HP-ENVY-060820/3900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue. **CVE ID : CVE-2020-12695**		
envy_4520_f0v63b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3901
envy_4520_f0v69a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3902
envy_4521_k9t10b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription	N/A	H-HP-ENVY-060820/3903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_4522_f0v67a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3904
envy_4523_j6u60b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3905
envy_4524_f0v71b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully	N/A	H-HP-ENVY-060820/3906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_4524_f0v72b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3907
envy_4524_k9t01a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3908
envy_4525_k9t09b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network	N/A	H-HP-ENVY-060820/3909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_4526_k9t05b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3910
envy_4527_j6u61b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3911
envy_4528_k9t08b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL	N/A	H-HP-ENVY-060820/3912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_5000_m2u85a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3913
envy_5000_m2u85b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3914
envy_5000_m2u91a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription	N/A	H-HP-ENVY-060820/3915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_5000_m2u94b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3916
envy_5000_z4a54a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3917
envy_5000_z4a74a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the	N/A	H-HP-ENVY-060820/3918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_5020_m2u91b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3919
envy_5530					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3920
envy_5531					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-	N/A	H-HP-ENVY-060820/3921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_5532					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3922
envy_5534					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3923
envy_5535					
Incorrect Default	08-06-2020	7.8	The Open Connectivity Foundation UPnP	N/A	H-HP-ENVY-060820/3924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_5536					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3925
envy_5539					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3926
envy_5540_f2e72a					
Incorrect	08-06-2020	7.8	The Open Connectivity	N/A	H-HP-ENVY-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Default Permissions			Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		060820/3927
envy_5540_g0v47a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3928
envy_5540_g0v51a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3929
envy_5540_g0v52a					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3930
envy_5540_g0v53a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3931
envy_5540_k7c85a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
envy_5541_k7g89a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3933
envy_5542_k7c88a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3934
envy_5543_n9u88a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue.	N/A	H-HP-ENVY-060820/3935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12695		
envy_5544_k7c89a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3936
envy_5544_k7c93a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3937
envy_5545_g0v50a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger	N/A	H-HP-ENVY-060820/3938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue. **CVE ID : CVE-2020-12695**		
envy_5546_k7c90a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3939
envy_5547_j6u64a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3940
envy_5548_k7g87a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription	N/A	H-HP-ENVY-060820/3941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_5640_b9s56a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3942
envy_5640_b9s58a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3943
envy_5642_b9s64a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully	N/A	H-HP-ENVY-060820/3944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_5643_b9s63a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3945
envy_5644_b9s65a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3946
envy_5646_f8b05a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network	N/A	H-HP-ENVY-060820/3947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_5664_f8b08a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3948
envy_5665_f8b06a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3949
envy_6020_5se16b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL	N/A	H-HP-ENVY-060820/3950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_6020_5se17a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3951
envy_6020_6wd35a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3952
envy_6020_7cz37a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription	N/A	H-HP-ENVY-060820/3953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
hp_envy_4520_f0v63a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/3954
hp_envy_4520_f0v63b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/3955
hp_envy_4520_f0v69a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the	N/A	H-HP-HP_E-060820/3956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
hp_envy_4521_k9t10b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/3957
hp_envy_4522_f0v67a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/3958
hp_envy_4523_j6u60b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-	N/A	H-HP-HP_E-060820/3959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
hp_envy_4524_f0v71b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/3960
hp_envy_4524_f0v72b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/3961
hp_envy_4524_k9t01a					
Incorrect Default	08-06-2020	7.8	The Open Connectivity Foundation UPnP	N/A	H-HP-HP_E-060820/3962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
hp_envy_4525_k9t09b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/3963
hp_envy_4526_k9t05b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/3964
hp_envy_4527_j6u61b					
Incorrect	08-06-2020	7.8	The Open Connectivity	N/A	H-HP-HP_E-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Default Permissions			Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		060820/3965
hp_envy_4528_k9t08b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/3966
hp_officejet_4650_e6g87a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_O-060820/3967
hp_officejet_4650_f1h96a					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_O-060820/3968
hp_officejet_4650_f1h96b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_O-060820/3969
hp_officejet_4652_f1j02a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_O-060820/3970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
hp_officejet_4652_f1j05b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_O-060820/3971
hp_officejet_4652_k9v84b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_O-060820/3972
hp_officejet_4654_f1j06b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue.	N/A	H-HP-HP_O-060820/3973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12695		
hp_officejet_4654_f1j07b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_O-060820/3974
hp_officejet_4655_f1j00a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_O-060820/3975
hp_officejet_4655_k9v79a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger	N/A	H-HP-HP_O-060820/3976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue. **CVE ID : CVE-2020-12695**		
hp_officejet_4655_k9v82b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_O-060820/3977
hp_officejet_4656_k9v81b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_O-060820/3978
hp_officejet_4657_v6d29b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription	N/A	H-HP-HP_O-060820/3979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
hp_officejet_4658_v6d30b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_O-060820/3980
officejet_4650_e6g87a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-OFFI-060820/3981
officejet_4650_f1h96a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully	N/A	H-HP-OFFI-060820/3982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
officejet_4650_f1h96b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-OFFI-060820/3983
officejet_4652_f1j02a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-OFFI-060820/3984
officejet_4652_f1j05b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network	N/A	H-HP-OFFI-060820/3985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
officejet_4652_k9v84b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-OFFI-060820/3986
officejet_4654_f1j06b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-OFFI-060820/3987
officejet_4654_f1j07b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL	N/A	H-HP-OFFI-060820/3988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
officejet_4655_f1j00a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-OFFI-060820/3989
officejet_4655_k9v79a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-OFFI-060820/3990
officejet_4655_k9v82b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription	N/A	H-HP-OFFI-060820/3991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
officejet_4656_k9v81b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-OFFI-060820/3992
officejet_4657_v6d29b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-OFFI-060820/3993
officejet_4658_v6d30b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the	N/A	H-HP-OFFI-060820/3994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
deskjet_ink_advantage_4536_f0v65a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-DESK-060820/3995
envy_100_cn519b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3996
deskjet_ink_advantage_4675_f1h97c					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-	N/A	H-HP-DESK-060820/3997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_110_cq812c					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3998
envy_4503_e6g71b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/3999
deskjet_ink_advantage_3546_a9t82a					
Incorrect Default	08-06-2020	7.8	The Open Connectivity Foundation UPnP	N/A	H-HP-DESK-060820/4000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_110_cq809d					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4001
envy_110_cq809a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4002
envy_114_cq812a					
Incorrect	08-06-2020	7.8	The Open Connectivity	N/A	H-HP-ENVY-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Default Permissions			Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		060820/4003
envy_4508_e6g72b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4004
envy_120_cz022b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4005
envy_4509_d3p94a					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4006
envy_4500_a9t89a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4007
envy_4511_k9h50a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
envy_4502_a9t85a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4009
envy_110_cq809b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4010
envy_110_cq809c					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue.	N/A	H-HP-ENVY-060820/4011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12695		
5660_f8b04a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-5660-060820/4012
5034_z4a74a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-5034-060820/4013
deskjet_ink_advantage_4515					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger	N/A	H-HP-DESK-060820/4014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue. **CVE ID : CVE-2020-12695**		
deskjet_ink_advantage_3548_a9t81b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-DESK-060820/4015
deskjet_ink_advantage_4518					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-DESK-060820/4016
deskjet_ink_advantage_4535_f0v64a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription	N/A	H-HP-DESK-060820/4017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
deskjet_ink_advantage_4535_f0v64c					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-DESK-060820/4018
deskjet_ink_advantage_4676_f1h98a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-DESK-060820/4019
envy_114_cq811b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully	N/A	H-HP-ENVY-060820/4020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_4505_a9t86a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4021
envy_4500_d3p93a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4022
envy_4501_c8d05a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network	N/A	H-HP-ENVY-060820/4023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_4502_a9t87b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4024
5020_z4a69a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-5020-060820/4025
5030_m2u92b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL	N/A	H-HP-5030-060820/4026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
deskjet_ink_advantage_3545_a9t81c					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-DESK-060820/4027
deskjet_ink_advantage_3545_a9t83b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-DESK-060820/4028
deskjet_ink_advantage_5575_g0v48c					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription	N/A	H-HP-DESK-060820/4029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
deskjet_ink_advantage_4538_f0v66b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-DESK-060820/4030
deskjet_ink_advantage_4675_f1h97a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-DESK-060820/4031
deskjet_ink_advantage_4675_f1h97b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the	N/A	H-HP-DESK-060820/4032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_100_cn517b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4033
envy_100_cn517a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4034
deskjet_ink_advantage_5575_g0v48b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-	N/A	H-HP-DESK-060820/4035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
deskjet_ink_advantage_4678_f1h99b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-DESK-060820/4036
deskjet_ink_advantage_4535_f0v64b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-DESK-060820/4037
envy_111_cq810a					
Incorrect Default	08-06-2020	7.8	The Open Connectivity Foundation UPnP	N/A	H-HP-ENVY-060820/4038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_114_cq811a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4039
deskjet_ink_advantage_3456_a9t84c					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-DESK-060820/4040
deskjet_ink_advantage_3545_a9t81a					
Incorrect	08-06-2020	7.8	The Open Connectivity	N/A	H-HP-DESK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Default Permissions			Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		060820/4041
envy_120_cz022a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4042
envy_4504_c8d04a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4043
envy_4507_e6g70b					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4044
envy_4504_a9t88b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4045
envy_120_cz022c					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
envy_4500_a9t80b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4047
envy_4500_a9t80a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4048
envy_4509_d3p94b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue.	N/A	H-HP-ENVY-060820/4049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12695		
envy_100_cn517c					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4050
envy_100_cn518a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4051
envy_100_cn519a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger	N/A	H-HP-ENVY-060820/4052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue. **CVE ID : CVE-2020-12695**		
5030_z4a70a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-5030-060820/4053
envy_6052_5se18a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4054
envy_6055_5se16a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription	N/A	H-HP-ENVY-060820/4055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_6540_b9s59a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4056
envy_7640					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4057
envy_7644_e4w46a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully	N/A	H-HP-ENVY-060820/4058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_7645_e4w44a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4059
envy_photo_6200_k7g18a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4060
envy_photo_6200_k7g26b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network	N/A	H-HP-ENVY-060820/4061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_photo_6200_k7s21b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4062
envy_photo_6200_y0k13d_					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4063
envy_photo_6200_y0k15a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL	N/A	H-HP-ENVY-060820/4064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_photo_6220_k7g20d					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4065
envy_photo_6220_k7g21b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4066
envy_photo_6222_y0k13d					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription	N/A	H-HP-ENVY-060820/4067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_photo_6222_y0k14d					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4068
envy_photo_6230_k7g25b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4069
envy_photo_6232_k7g26b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the	N/A	H-HP-ENVY-060820/4070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_photo_6234_k7s21b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4071
envy_photo_6252_k7g22a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4072
envy_photo_7100_3xd89a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-	N/A	H-HP-ENVY-060820/4073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_photo_7100_k7g93a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4074
envy_photo_7100_k7g99a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4075
envy_photo_7100_z3m37a					
Incorrect Default	08-06-2020	7.8	The Open Connectivity Foundation UPnP	N/A	H-HP-ENVY-060820/4076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_photo_7100_z3m52a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4077
envy_photo_7120_z3m41d					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4078
envy_photo_7155_z3m52a					
Incorrect	08-06-2020	7.8	The Open Connectivity	N/A	H-HP-ENVY-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Default Permissions			Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		060820/4079
envy_photo_7164_k7g99a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4080
envy_photo_7800_k7r96a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4081
envy_photo_7800_k7s00a					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4082
envy_photo_7800_k7s10d					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4083
envy_photo_7800_y0g42d					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
envy_photo_7800_y0g52b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4085
envy_photo_7822_y0g42d					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4086
envy_photo_7822_y0g43d					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue.	N/A	H-HP-ENVY-060820/4087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12695		
envy_photo_7830_y0g50b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4088
envy_pro_6420_5se45b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4089
envy_pro_6420_5se46a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger	N/A	H-HP-ENVY-060820/4090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue. **CVE ID : CVE-2020-12695**		
envy_pro_6420_6wd14a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4091
envy_pro_6420_6wd16a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4092
envy_pro_6452_5se47a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription	N/A	H-HP-ENVY-060820/4093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
envy_pro_6455_5se45a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-ENVY-060820/4094
hp_deskjet_ink_advantage_4535_f0v64a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_D-060820/4095
hp_deskjet_ink_advantage_4535_f0v64b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully	N/A	H-HP-HP_D-060820/4096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
hp_deskjet_ink_advantage_4535_f0v64c					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_D-060820/4097
hp_deskjet_ink_advantage_4536_f0v65a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_D-060820/4098
hp_deskjet_ink_advantage_4538_f0v66b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network	N/A	H-HP-HP_D-060820/4099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
hp_deskjet_ink_advantage_4675_f1h97a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_D-060820/4100
hp_deskjet_ink_advantage_4675_f1h97b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_D-060820/4101
hp_deskjet_ink_advantage_4675_f1h97c					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL	N/A	H-HP-HP_D-060820/4102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
hp_deskjet_ink_advantage_4676_f1h98a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_D-060820/4103
hp_deskjet_ink_advantage_4678_f1h99b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_D-060820/4104
hp_envy_4511_k9h50a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription	N/A	H-HP-HP_E-060820/4105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
hp_envy_4512_k9h49a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/4106
hp_envy_4513_k9h51a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/4107
hp_envy_4516_k9h52a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the	N/A	H-HP-HP_E-060820/4108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
hp_envy_4520_e6g67a					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/4109
hp_envy_4520_e6g67b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HP-HP_E-060820/4110
Huawei					
honor_view_20					
Improper Handling of	05-06-2020	5	Huawei Smartphones HONOR 20 PRO;Honor View	N/A	H-HUA-HONO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			20;HONOR 20 have an improper handling of exceptional condition Vulnerability. A component cannot deal with an exception correctly. Attackers can exploit this vulnerability by sending malformed message. This could compromise normal service of affected phones. **CVE ID : CVE-2020-9074**		060820/4111
honor_20					
Improper Handling of Exceptional Conditions	05-06-2020	5	Huawei Smartphones HONOR 20 PRO;Honor View 20;HONOR 20 have an improper handling of exceptional condition Vulnerability. A component cannot deal with an exception correctly. Attackers can exploit this vulnerability by sending malformed message. This could compromise normal service of affected phones. **CVE ID : CVE-2020-9074**	N/A	H-HUA-HONO-060820/4112
honor_20_pro					
Improper Handling of Exceptional Conditions	05-06-2020	5	Huawei Smartphones HONOR 20 PRO;Honor View 20;HONOR 20 have an improper handling of exceptional condition Vulnerability. A component cannot deal with an exception correctly. Attackers can exploit this vulnerability by sending malformed message. This	N/A	H-HUA-HONO-060820/4113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could compromise normal service of affected phones. **CVE ID : CVE-2020-9074**		
hg532e					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-HUA-HG53-060820/4114
ar510					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	H-HUA-AR51-060820/4115
usg6300e					
Information Exposure	15-06-2020	4	Huawei products Secospace USG6300;USG6300E with	N/A	H-HUA-USG6-060820/4116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions of V500R001C30,V500R001C50,V500R001C60,V500R001C80,V500R005C00,V500R005C10;V600R006C00 have a vulnerability of insufficient input verification. An attacker with limited privilege can exploit this vulnerability to access a specific directory. Successful exploitation of this vulnerability may lead to information leakage. **CVE ID : CVE-2020-9075**		
ips_module					
Improper Authentication	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability.	N/A	H-HUA-IPS_-060820/4117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**		
ar120-s					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	H-HUA-AR12-060820/4118
ar1200					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions	N/A	H-HUA-AR12-060820/4119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**		
ar1200-s					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	H-HUA-AR12-060820/4120
tony-al00b					
Improper Authentication	15-06-2020	4	HUAWEI P30;HUAWEI P30 Pro;Tony-AL00B smartphones with versions earlier than 10.1.0.135(C00E135R2P11); versions earlier than 10.1.0.135(C00E135R2P8), versions earlier than 10.1.0.135 have an improper authentication vulnerability. Due to the identity of the message sender not being properly verified, an attacker can exploit this vulnerability through man-in-the-middle attack to	N/A	H-HUA-TONY-060820/4121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			induce user to access malicious URL. **CVE ID : CVE-2020-9076**		
nip6300					
Improper Authentication	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**	N/A	H-HUA-NIP6-060820/4122
nip6600					
Improper Authentication	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace	N/A	H-HUA-NIP6-060820/4123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**		
nip6800					
Missing Release of Resource after Effective Lifetime	05-06-2020	4	Huawei products NIP6800;Secospace USG6600;USG9500 have a memory leak vulnerability. An attacker with high privileges exploits this vulnerability by continuously performing specific operations. Successful exploitation of this vulnerability can cause service abnormal. **CVE ID : CVE-2020-1883**	N/A	H-HUA-NIP6-060820/4124
Improper Authenticati on	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace	N/A	H-HUA-NIP6-060820/4125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**		
secospace_usg6300					
Information Exposure	15-06-2020	4	Huawei products Secospace USG6300;USG6300E with versions of V500R001C30,V500R001C50,V500R001C60,V500R001C80,V500R005C00,V500R005C10;V600R006C00 have a vulnerability of insufficient input verification. An attacker with limited privilege can exploit this vulnerability to access a specific directory. Successful exploitation of this vulnerability may lead to	N/A	H-HUA-SECO-060820/4126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information leakage. **CVE ID : CVE-2020-9075**		
Improper Authentication	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**	N/A	H-HUA-SECO-060820/4127
secospace_usg6500					
Improper Authentication	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20;	N/A	H-HUA-SECO-060820/4128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**		
secospace_usg6600					
Missing Release of Resource after Effective Lifetime	05-06-2020	4	Huawei products NIP6800;Secospace USG6600;USG9500 have a memory leak vulnerability. An attacker with high privileges exploits this vulnerability by continuously performing specific operations. Successful exploitation of this vulnerability can cause service abnormal. **CVE ID : CVE-2020-1883**	N/A	H-HUA-SECO-060820/4129
Improper Authenticati on	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with	N/A	H-HUA-SECO-060820/4130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**		
p30_pro					
Improper Authentication	15-06-2020	4	HUAWEI P30;HUAWEI P30 Pro;Tony-AL00B smartphones with versions earlier than 10.1.0.135(C00E135R2P11); versions earlier than 10.1.0.135(C00E135R2P8), versions earlier than 10.1.0.135 have an improper authentication vulnerability. Due to the identity of the message sender not being properly verified, an attacker can exploit this vulnerability through man-in-the-middle attack to induce user to access malicious URL.	N/A	H-HUA-P30_-060820/4131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9076		
p30					
Improper Authenticati on	15-06-2020	4	HUAWEI P30;HUAWEI P30 Pro;Tony-AL00B smartphones with versions earlier than 10.1.0.135(C00E135R2P11); versions earlier than 10.1.0.135(C00E135R2P8), versions earlier than 10.1.0.135 have an improper authentication vulnerability. Due to the identity of the message sender not being properly verified, an attacker can exploit this vulnerability through man-in-the-middle attack to induce user to access malicious URL. **CVE ID : CVE-2020-9076**	N/A	H-HUA-P30-060820/4132
Improper Authenticati on	15-06-2020	4.6	HUAWEI P30 smart phone with versions earlier than 10.1.0.135(C00E135R2P11) have an improper authentication vulnerability. Due to improper authentication of specific interface, in specific scenario attackers could access specific interface without authentication. Successful exploit could allow the attacker to perform unauthorized operations. **CVE ID : CVE-2020-1813**	N/A	H-HUA-P30-060820/4133
hg255s					
Incorrect Default	08-06-2020	7.8	The Open Connectivity Foundation UPnP	N/A	H-HUA-HG25-060820/4134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
ar150					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	H-HUA-AR15-060820/4135
ar150-s					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending	N/A	H-HUA-AR15-060820/4136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**		
ar160					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	H-HUA-AR16-060820/4137
ar200					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the	N/A	H-HUA-AR20-060820/4138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**		
ar200-s					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	H-HUA-AR20-060820/4139
ar2200					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit	N/A	H-HUA-AR22-060820/4140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200 R007C00SPCa00 **CVE ID : CVE-2020-9071**		
ar2200-s					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200 R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	H-HUA-AR22-060820/4141
ar3200					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal	N/A	H-HUA-AR32-060820/4142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**		
ar3600					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	H-HUA-AR36-060820/4143
netengine16ex					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected	N/A	H-HUA-NETE-060820/4144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**		
srg1300					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	H-HUA-SRG1-060820/4145
srg2300					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions	N/A	H-HUA-SRG2-060820/4146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include:AR120-S versions V200R007C00SPC900,V200 R007C00SPCa00 **CVE ID : CVE-2020-9071**		
srg3300					
Out-of-bounds Read	01-06-2020	4	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200 R007C00SPCa00 **CVE ID : CVE-2020-9071**	N/A	H-HUA-SRG3-060820/4147
ngfw_module					
Improper Authenticati on	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80; V500R005C00; V500R005C10;	N/A	H-HUA-NGFW-060820/4148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**		
usg9500					
Missing Release of Resource after Effective Lifetime	05-06-2020	4	Huawei products NIP6800;Secospace USG6600;USG9500 have a memory leak vulnerability. An attacker with high privileges exploits this vulnerability by continuously performing specific operations. Successful exploitation of this vulnerability can cause service abnormal. **CVE ID : CVE-2020-1883**	N/A	H-HUA-USG9-060820/4149
Improper Authenticati on	08-06-2020	7.5	Huawei products IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG9500 with versions of V500R001C00; V500R001C20; V500R001C30; V500R001C50; V500R001C60; V500R001C80;	N/A	H-HUA-USG9-060820/4150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00; V500R005C10; V500R005C20; V500R002C00; V500R002C10; V500R002C20; V500R002C30 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device. **CVE ID : CVE-2020-9099**		
Intel					
core_i3-3120m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4151
core_i3-3120me					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4152
core_i3-3130m					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4153
core_i3-3210					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4154
core_i3-3217u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4155
core_i3-3217ue					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i3-3220					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4157
core_i3-3220t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4158
core_i3-3225					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4159
core_i3-3227u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i3-3229y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4161
core_i3-3240					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4162
core_i3-3240t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4163
core_i3-3245					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i3-3250					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4165
core_i3-3250t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4166
core_i3-4005u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4167
core_i3-4010u					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4168
core_i3-4010y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4169
core_i3-4012y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4170
core_i3-4020y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i3-4025u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4172
core_i3-4030u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4173
core_i3-4030y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4174
core_i3-4100m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i3-4100u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4176
core_i3-4110m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4177
core_i3-4120u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4178
core_i3-4130					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i3-4130t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4180
core_i3-4150					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4181
core_i3-4150t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4182
core_i3-4158u					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4183
core_i3-4160					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4184
core_i3-4160t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4185
core_i3-4170					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i3-4170t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4187
core_i3-4330					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4188
core_i3-4330t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4189
core_i3-4340					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i3-4350					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4191
core_i3-4350t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4192
core_i3-4360					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4193
core_i3-4360t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i3-4370					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4195
core_i3-4370t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4196
core_i3-5006u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4197
core_i5-3210m					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4198
core_i5-3230m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4199
core_i5-3317u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4200
core_i5-3320m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-3330					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4202
core_i5-3330s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4203
core_i5-3337u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4204
core_i5-3339y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i5-3340					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4206
core_i5-3340m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4207
core_i5-3340s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4208
core_i5-3350p					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-3360m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4210
core_i5-3380m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4211
core_i5-3427u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4212
core_i5-3437u					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4213
core_i5-3439y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4214
core_i5-3450					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4215
core_i5-3450s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-3470					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4217
core_i5-3470s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4218
core_i5-3470t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4219
core_i5-3475s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i5-3550					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4221
core_i5-3550s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4222
core_i5-3570					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4223
core_i5-3570k					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-3570s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4225
core_i5-3570t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4226
core_i5-3610me					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4227
core_i5-4200u					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4228
core_i5-4200y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4229
core_i5-4202y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4230
core_i5-4210h					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-4210u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4232
core_i5-4210y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4233
core_i5-4220y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4234
core_i5-4250u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i5-4258u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4236
core_i5-4260u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4237
core_i5-4278u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4238
core_i5-4288u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-4300u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4240
core_i5-4300y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4241
core_i5-4302y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4242
core_i5-4308u					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4243
core_i5-4350u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4244
core_i5-4402ec					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4245
core_i5-4430					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-4430s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4247
core_i5-4440					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4248
core_i5-4440s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4249
core_i5-4460					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i5-4460s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4251
core_i5-4460t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4252
core_i5-4570					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4253
core_i5-4570r					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-4570s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4255
core_i5-4570t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4256
core_i5-4590					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4257
core_i5-4590s					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4258
core_i5-4590t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4259
core_i5-4670					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4260
core_i5-4670k					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-4670r					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4262
core_i5-4670s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4263
core_i5-4670t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4264
core_i5-4690					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i5-4690s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4266
core_i5-4690t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4267
core_i5-5350					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4268
core_i5-5575r					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-5675c					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4270
core_i5-5675r					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4271
core_i7-3517u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4272
core_i7-3517ue					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4273
core_i7-3520m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4274
core_i7-3537u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4275
core_i7-3540m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-3555le					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4277
core_i7-3610qe					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4278
core_i7-3610qm					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4279
core_i7-3612qe					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i7-3612qm					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4281
xeon_e3-1260l_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4282
xeon_e3-1240l_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4283
xeon_e3-1235l_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-XEON-060820/4284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
xeon_e3-1245_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4285
xeon_e3-1240_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4286
xeon_e3-1230_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4287
xeon_e3-1225_v5					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4288
xeon_e3-1220_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4289
xeon_e3-1535m_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4290
xeon_e3-1505m_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xeon_e3-1505l_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4292
xeon_e3-1501l_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4293
xeon_e3-1501m_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4294
xeon_e3-1285_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-XEON-060820/4295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
xeon_e3-1280_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4296
xeon_e3-1275_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4297
xeon_e3-1270_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4298
xeon_e3-1245_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-XEON-060820/4299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
xeon_e3-1240_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4300
xeon_e3-1230_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4301
xeon_e3-1225_v6					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4302
xeon_e3-1220_v6					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4303
xeon_e-2288g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4304
xeon_e-2286m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4305
xeon_e-2278gel					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xeon_e-2278ge					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4307
xeon_e-2278g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4308
core_i5-9600kf					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4309
core_i5-9400f					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i3-5015u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4311
core_i3-5020u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4312
core_i3-5005u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4313
core_i3-5010u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i3-5157u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4315
core_m3-8100y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4316
core_m3-7y30					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4317
core_m5-6y54					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4318
core_m3-6y30					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4319
core_m-5y51					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4320
core_m-5y10c					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_m-5y10					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4322
core_m-5y10a					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4323
core_i7-4860hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4324
core_i7-4870hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i7-4900mq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4326
core_i7-4910mq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4327
core_i7-4950hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4328
core_i7-4960hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i7-4980hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4330
core_i7-5700eq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4331
core_i7-5775r					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4332
core_i7-5850eq					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4333
core_m-5y3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4334
pentium_1405_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4335
pentium_2020m_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pentium_2030m_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4337
pentium_2117u_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4338
pentium_2127u_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4339
pentium_2129y_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-PENT-060820/4340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
pentium_3205u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4341
pentium_3215u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4342
pentium_3556u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4343
pentium_3558u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-PENT-060820/4344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
pentium_3560y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4345
pentium_3561y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4346
pentium_3665u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4347
pentium_3765u					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-PENT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4348
pentium_a1018_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4349
pentium_b915c					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4350
pentium_b925c					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pentium_g2010_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4352
pentium_g2020_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4353
pentium_g2020t_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4354
pentium_g2030_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-PENT-060820/4355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
pentium_g2030t_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4356
pentium_g2100t_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4357
pentium_g2120_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4358
pentium_g2120t_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-PENT-060820/4359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
pentium_g2130_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4360
pentium_g2140_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4361
pentium_g3220					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4362
pentium_g3220t					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-PENT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4363
pentium_g3240					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4364
pentium_g3240t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4365
pentium_g3250					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pentium_g3250t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4367
pentium_g3258					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4368
pentium_g3260					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4369
pentium_g3260t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-PENT-060820/4370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
pentium_g3420t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4371
pentium_g3430					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4372
pentium_g3440					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4373
pentium_g3440t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-PENT-060820/4374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
pentium_g3450					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4375
pentium_g3450t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4376
pentium_g3460					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4377
pentium_g3460t					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-PENT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4378
pentium_g3470					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4379
xeon_e3-1105c					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4380
xeon_e3-1125c					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-10700f					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4382
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4383
core_i7-10700e					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4384
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation	N/A	H-INT-CORE-060820/4385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-10700					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4386
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4387
core_i7-10610u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4388
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an	N/A	H-INT-CORE-060820/4389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-1060g7					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4390
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4391
core_i7-1068ng7					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4392
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R)	N/A	H-INT-CORE-060820/4393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
celeron_g4900					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4394
celeron_g3920					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4395
celeron_g3902e					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4396
celeron_g3900te					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4397
celeron_g3900t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4398
celeron_g3900					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4399
core_i7-8510y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	N/A	H-INT-CORE-060820/4400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0543		
core_i5-8210y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4401
core_i5-8310y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4402
core_i5-6500t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4403
core_i5-6600					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable	N/A	H-INT-CORE-060820/4404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-6600t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4405
core_i5-6440eq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4406
core_i5-6442eq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4407
core_i5-6500te					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R)	N/A	H-INT-CORE-060820/4408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-10110y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4409
celeron_5305u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4410
core_i7-9850h					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4411
core_i7-9700kf					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4412
core_i7-9700k					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4413
xeon_e3-1585_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4414
xeon_e3-1585l_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	N/A	H-INT-XEON-060820/4415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0543		
xeon_e3-1578l_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4416
xeon_e3-1575m_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4417
xeon_e3-1565l_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4418
xeon_e3-1558l_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable	N/A	H-INT-XEON-060820/4419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure via local access. **CVE ID : CVE-2020-0543**		
xeon_e3-1545m_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4420
xeon_e3-1535m_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4421
xeon_e3-1515m_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4422
xeon_e3-1505m_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R)	N/A	H-INT-XEON-060820/4423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
xeon_e3-1505l_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4424
xeon_e3-1280_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4425
xeon_e3-1275_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4426
xeon_e3-1270_v5					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4427
xeon_e3-1268l_v5					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4428
core_i7-8665ue					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4429
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access.	N/A	H-INT-CORE-060820/4430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0529		
core_i7-8665u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4431
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4432
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4433
core_i7-8557u					
Improper Restriction of Operations within the Bounds of a Memory	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation	N/A	H-INT-CORE-060820/4434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4435
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4436
core_i7-8850h					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4437
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to	N/A	H-INT-CORE-060820/4438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4439
core_i7-8809g					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4440
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4441
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable	N/A	H-INT-CORE-060820/4442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i7-8750h					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4443
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4444
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4445
core_i7-8709g					
Improper Restriction of Operations within the	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an	N/A	H-INT-CORE-060820/4446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4447
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4448
core_i7-8706g					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4449
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families	N/A	H-INT-CORE-060820/4450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4451
core_i7-8705g					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4452
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4453
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i7-8700t					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4455
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4456
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4457
core_i7-8700k					
Improper Restriction of	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation	N/A	H-INT-CORE-060820/4458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4459
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4460
core_i7-8700b					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4461
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th	N/A	H-INT-CORE-060820/4462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4463
core_i7-8700					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4464
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4465
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read	N/A	H-INT-CORE-060820/4466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i7\+8700					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4467
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4468
core_i7-8569u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4470
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4471
core_i7-8650u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4472
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4474
core_i7-8565u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4475
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4476
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-8559u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4478
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4479
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4480
core_i7-8550u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of	N/A	H-INT-CORE-060820/4481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4482
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4483
core_i7-8500y					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4484
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation	N/A	H-INT-CORE-060820/4485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2020-0529**		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4486
core_i7-8086k					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4487
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4488
core_i9-9980hk					
Improper Restriction of Operations within the Bounds of a	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to	N/A	H-INT-CORE-060820/4489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4490
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4491
core_i9-9880h					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4492
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an	N/A	H-INT-CORE-060820/4493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4494
core_i9-9900t					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4495
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4496
core_i9-9900ks					
Improper Restriction of Operations	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor	N/A	H-INT-CORE-060820/4497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4498
core_i9-9900kf					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4499
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4500
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R)	N/A	H-INT-CORE-060820/4501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i9-9900k					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4502
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4503
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4504
core_i9-9900					
Improper Restriction	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th,	N/A	H-INT-CORE-060820/4505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4506
celeron_g4950					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4507
celeron_g4930					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4508
celeron_g4920					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4509
celeron_g4900t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4510
celeron_g3930te					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4511
celeron_g3930e					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	N/A	H-INT-CELE-060820/4512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0543		
xeon_e3-1268l_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4513
xeon_e3-1271_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4514
xeon_e3-1275_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4515
xeon_e3-1246_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable	N/A	H-INT-XEON-060820/4516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure via local access. **CVE ID : CVE-2020-0543**		
xeon_e3-1245_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4517
xeon_e3-1241_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4518
xeon_e3-1240l_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4519
xeon_e3-1240_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R)	N/A	H-INT-XEON-060820/4520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
xeon_e3-1231_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4521
xeon_e3-1230l_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4522
xeon_e3-1230_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4523
xeon_e3-1226_v3					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4524
xeon_e3-1225_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4525
xeon_e3-1220l_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4526
xeon_e3-1220_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	N/A	H-INT-XEON-060820/4527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0543		
xeon_e3-1285_v4					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4528
xeon_e3-1278l_v4					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4529
xeon_e3-1265l_v4					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4530
xeon_e3-1258l_v4					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable	N/A	H-INT-XEON-060820/4531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure via local access. **CVE ID : CVE-2020-0543**		
ssd_d3-s4510					
Information Exposure	15-06-2020	2.1	Insufficient control flow management in firmware for some Intel(R) Data Center SSDs may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0527**	N/A	H-INT-SSD_-060820/4532
ssd_dc_p4510					
Information Exposure	15-06-2020	2.1	Insufficient control flow management in firmware for some Intel(R) Data Center SSDs may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0527**	N/A	H-INT-SSD_-060820/4533
ssd_dc_p4610					
Information Exposure	15-06-2020	2.1	Insufficient control flow management in firmware for some Intel(R) Data Center SSDs may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0527**	N/A	H-INT-SSD_-060820/4534
core_i7-6970hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable	N/A	H-INT-CORE-060820/4535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i7-6920hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4536
core_i7-6870hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4537
core_i7-6822eq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4538
core_i7-6820hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R)	N/A	H-INT-CORE-060820/4539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i7-6820hk					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4540
core_i7-6820eq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4541
core_i7-6700k					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4542
core_i7-6700t					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4543
core_i7-6700te					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4544
core_i7-6700					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4545
core_i7-6770hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	N/A	H-INT-CORE-060820/4546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0543		
core_i7-6700hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4547
core_i7-6660u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4548
core_i7-6650u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4549
core_i7-6600u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable	N/A	H-INT-CORE-060820/4550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i7-6567u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4551
core_i7-6560u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4552
core_i7-6500u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4553
core_i5-7600k					
Improper Restriction of	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation	N/A	H-INT-CORE-060820/4554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4555
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4556
core_i5-7600t					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4557
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th	N/A	H-INT-CORE-060820/4558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4559
core_i5-7600					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4560
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4561
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read	N/A	H-INT-CORE-060820/4562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-7500					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4563
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4564
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4565
core_i7-3615qe					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4566
core_i7-3615qm					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4567
core_i7-3630qm					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4568
core_i7-3632qm					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-3635qm					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4570
core_i7-3667u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4571
core_i7-3687u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4572
core_i7-3689y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i7-3720qm					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4574
core_i7-3740qm					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4575
core_i7-3770					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4576
core_i7-3770k					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i7-3770s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4578
core_i7-3770t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4579
core_i7-3820qm					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4580
core_i7-3920xm					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4581
core_i7-3940xm					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4582
core_i7-4500u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4583
core_i7-4510u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-4550u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4585
core_i7-4558u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4586
core_i7-4578u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4587
core_i7-4600u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i7-4610y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4589
core_i7-4650u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4590
core_i7-4700ec					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4591
core_i7-4700eq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i7-4700hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4593
core_i7-4700mq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4594
core_i7-4702ec					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4595
core_i7-4702hq					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4596
core_i7-4702mq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4597
core_i7-4710hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4598
core_i7-4710mq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-4712hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4600
core_i7-4712mq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4601
core_i7-4720hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4602
core_i7-4722hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i7-4750hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4604
core_i7-4760hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4605
core_i7-4765t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4606
core_i7-4770					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i7-4770hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4608
core_i7-4770k					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4609
core_i7-4770r					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4610
core_i7-4770s					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4611
core_i7-4770t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4612
core_i7-4771					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4613
core_i7-4785t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-4790					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4615
core_i7-4790s					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4616
core_i7-4790t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4617
core_i7-4800mq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i7-4810mq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4619
core_i7-4850hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4620
core_i9-8950hk					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4621
core_i7-1065g7					
Improper Restriction of Operations	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor	N/A	H-INT-CORE-060820/4622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4623
core_i7-5850hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4624
core_i7-5950hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4625
core_i7-5775c					
Information	15-06-2020	2.1	Incomplete cleanup from specific special register read	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4626
core_i7-5700hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4627
core_i7-5750hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4628
core_i7-5500u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-5550u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4630
core_i7-5557u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4631
core_i5-10210u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4632
core_i5-10310y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i5-10210y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4634
xeon_e3-1221_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4635
xeon_e3-1235_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4636
xeon_e3-1265l					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-XEON-060820/4637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i7-7740x					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4638
core_i7-8670					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4639
core_i7-8670t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4640
core_i5-8420					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4641
core_i5-8420t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4642
core_i5-8550					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4643
core_i5-8650					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i3-8000t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4645
core_i3-8000					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4646
core_i3-8020					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4647
core_i3-8100h					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i3-8120					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4649
pentium_g5400					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4650
pentium_g5400t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4651
pentium_g5420					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-PENT-060820/4652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
pentium_g5420t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4653
pentium_g5500					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4654
pentium_g5500t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4655
pentium_g5600					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-PENT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4656
xeon_e-2284g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4657
xeon_e-2184g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4658
core_i5-8650k					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i3-7020u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4660
core_i5-7500t					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4661
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4662
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	N/A	H-INT-CORE-060820/4663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0543		
core_i5-7442eq					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4664
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4665
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4666
core_i5-7440hq					
Improper Restriction of Operations within the Bounds of a Memory	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation	N/A	H-INT-CORE-060820/4667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4668
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4669
core_i5-7440eq					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4670
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to	N/A	H-INT-CORE-060820/4671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4672
core_i5-7400t					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4673
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4674
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable	N/A	H-INT-CORE-060820/4675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-7400					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4676
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4677
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4678
core_i5-7360u					
Improper Restriction of Operations within the	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an	N/A	H-INT-CORE-060820/4679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4680
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4681
core_i5-7300u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4682
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families	N/A	H-INT-CORE-060820/4683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4684
core_i5-7300hq					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4685
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4686
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-7287u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4688
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4689
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4690
core_i5-7267u					
Improper Restriction of	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation	N/A	H-INT-CORE-060820/4691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4692
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4693
core_i5-7260u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4694
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th	N/A	H-INT-CORE-060820/4695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4696
core_i5-7200u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4697
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4698
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read	N/A	H-INT-CORE-060820/4699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-7y54					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4700
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4701
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4702
core_i5-7y57					
Improper	15-06-2020	4.6	Improper buffer restrictions	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		060820/4703
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4704
core_i7-7920hq					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4705
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4707
core_i7-7820hq					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4708
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4709
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-7820hk					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4711
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4712
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4713
core_i7-7820eq					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of	N/A	H-INT-CORE-060820/4714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4715
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4716
core_i7-7700hq					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4717
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation	N/A	H-INT-CORE-060820/4718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2020-0529**		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4719
core_i7-7700k					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4720
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4721
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i7-7700t					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4723
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4724
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4725
core_i7-7660u					
Improper Restriction of Operations within the Bounds of a	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to	N/A	H-INT-CORE-060820/4726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4727
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4728
core_i7-7600u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4729
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an	N/A	H-INT-CORE-060820/4730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4731
core_i7-7567u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4732
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4733
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to	N/A	H-INT-CORE-060820/4734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i7-7560u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4735
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4736
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4737
core_i7-7500u					
Improper Restriction of Operations	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor	N/A	H-INT-CORE-060820/4738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4739
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4740
core_i7-7y75					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4741
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R)	N/A	H-INT-CORE-060820/4742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4743
core_i3-8130u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4744
core_i3-7100e					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4745
core_i3-7101e					
Information	15-06-2020	2.1	Incomplete cleanup from specific special register read	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4746
core_i3-7101te					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4747
core_i3-7102e					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4748
core_i3-7120					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i3-7120t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4750
core_i3-7320t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4751
core_i3-7340					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4752
core_i7-7510u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i5-7210u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4754
core_i5-7500u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4755
core_i3-7007u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4756
core_i3-7110u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i3-7130u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4758
pentium_4415u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4759
celeron_3865u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4760
celeron_3965u					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CELE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4761
core_i5-7640x					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4762
xeon_e3-1270					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4763
core_i5-9400					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-8265u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4765
core_i5-8200y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4766
core_i5-8400t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4767
core_i5-8300h					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i5-8259u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4769
core_i5-8400b					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4770
core_i5-8500b					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4771
core_i5-8305g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-8400					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4773
core_i5-8250u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4774
core_i5-6350hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4775
core_i5-6200u					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4776
core_i5-6300hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4777
core_i5-6287u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4778
core_i5-6267u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-6260u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4780
core_i5-5200u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4781
core_i5-5287u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4782
core_i5-5250u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i5-5257u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4784
core_4205u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4785
core_5405u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4786
core_8269u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_9300h					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4788
core_9750hf					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4789
core_i7-8560u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4790
pentium_gold_6405u					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-PENT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4791
core_i7-10710u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4792
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4793
core_i7-10510u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access.	N/A	H-INT-CORE-060820/4794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0528		
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4795
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4796
core_i7-10510y					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4797
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access.	N/A	H-INT-CORE-060820/4798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0529		
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4799
core_i5-9400h					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4800
core_i5-8365u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4801
core_i5-9600k					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i5-8600t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4803
core_i5-8400h					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4804
core_i5-8600					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4805
core_i5-8500					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i5-8500t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4807
core_i5-8600k					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4808
core_i5-8350u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4809
core_m7-6y75					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4810
core_i5-6300u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4811
core_i5-6500					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4812
core_m5-6y57					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-6440hq					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4814
core_i3-8145u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4815
core_i3-8300					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4816
core_i3-8100t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i3-8300t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4818
core_i3-8109u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4819
core_i3-8100					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4820
core_i3-8350k					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i3-7167u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4822
core_i3-7100h					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4823
core_i3-7100u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4824
core_i3-6100u					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4825
core_i3-6100h					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4826
core_i3-6167u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4827
core_i3-6100					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
celeron_3965y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4829
core_i5-6400					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4830
core_i5-6400t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4831
core_i5-6600k					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i3-6100e					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4833
core_i3-6100t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4834
core_i3-6100te					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4835
core_i3-6102e					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
core_i3-6120					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4837
core_i3-6120t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4838
core_i3-6300					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4839
core_i3-6300t					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4840
core_i3-6320					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4841
core_i3-6320t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4842
pentium_g4400t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pentium_g4400te					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4844
pentium_g4420					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4845
pentium_g4420t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4846
pentium_g4500					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-PENT-060820/4847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
pentium_g4500t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4848
pentium_g4520					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4849
pentium_g4520t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4850
pentium_g4540					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-PENT-060820/4851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
celeron_g3920t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4852
celeron_g3940					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4853
core_i7-6510u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4854
core_i5-6210u					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4855
core_i5-6310u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4856
core_i3-6110u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4857
celeron_3855u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
celeron_3955u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4859
celeron_1000m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4860
celeron_1005m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4861
celeron_1007u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CELE-060820/4862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
celeron_1017u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4863
celeron_1019y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4864
celeron_1020e					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4865
celeron_1020m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CELE-060820/4866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
celeron_1037u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4867
celeron_1047ue					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4868
celeron_2955u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4869
celeron_2957u					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CELE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4870
celeron_2970m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4871
celeron_2980u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4872
celeron_2981u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
celeron_3765u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4874
celeron_725c					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4875
celeron_927ue					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4876
celeron_g1610					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CELE-060820/4877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
celeron_g1610t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4878
celeron_g1620					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4879
celeron_g1620t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4880
celeron_g1630					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CELE-060820/4881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
celeron_g1820					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4882
celeron_g1820t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4883
celeron_g1830					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4884
celeron_g1840					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CELE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4885
celeron_g1840t					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4886
celeron_g1850					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4887
core_i3-2115c					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i3-3110m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4889
core_i3-3115c					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4890
core_i5-6360u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4891
core_i7-5600u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-CORE-060820/4892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
core_i5-5350u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4893
core_i7-5650u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4894
core_m-5y71					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4895
core_m-5y70					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-CORE-060820/4896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
xeon_e3-1290_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4897
xeon_e3-1280_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4898
xeon_e3-1275_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4899
xeon_e3-1270_v2					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4900
xeon_e3-1265l_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4901
xeon_e3-1245_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4902
xeon_e3-1240_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xeon_e3-1230_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4904
xeon_e3-1225_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4905
xeon_e3-1220_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4906
xeon_e3-1220l_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-XEON-060820/4907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
xeon_e3-1125c_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4908
xeon_e3-1105c_v2					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4909
xeon_e3-1286l_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4910
xeon_e3-1286_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-XEON-060820/4911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
xeon_e3-1285l_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4912
xeon_e3-1285_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4913
xeon_e3-1281_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4914
xeon_e3-1280_v3					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4915
xeon_e3-1276_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4916
xeon_e3-1275l_v3					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4917
innovation_engine					
Improper Privilege Management	15-06-2020	4.6	Insufficient control flow management in firmware build and signing tool for Intel(R) Innovation Engine before version 1.0.859 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	N/A	H-INT-INNO-060820/4918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8675		
core_i7-10875h					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4919
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4920
core_i7-10850h					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4921
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to	N/A	H-INT-CORE-060820/4922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-10810u					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4923
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4924
core_i7-10750h					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4925
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families	N/A	H-INT-CORE-060820/4926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-10700te					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4927
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4928
core_i7-10700t					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4929
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th	N/A	H-INT-CORE-060820/4930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**		
core_i7-10700kf					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4931
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4932
core_i7-10700k					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4934
xeon_e-2276ml					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4935
xeon_e-2276me					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4936
xeon_e-2276m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	N/A	H-INT-XEON-060820/4937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0543		
xeon_e-2276g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4938
xeon_e-2274g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4939
xeon_e-2254ml					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4940
xeon_e-2254me					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable	N/A	H-INT-XEON-060820/4941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure via local access. **CVE ID : CVE-2020-0543**		
xeon_e-2246g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4942
xeon_e-2244g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4943
xeon_e-2236					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4944
xeon_e-2234					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R)	N/A	H-INT-XEON-060820/4945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
xeon_e-2226ge					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4946
xeon_e-2226g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4947
xeon_e-2224					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4948
xeon_e-2224g					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4949
xeon_e-2186g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4950
xeon_e-2186m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4951
xeon_e-2176g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	N/A	H-INT-XEON-060820/4952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0543		
xeon_e-2176m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4953
xeon_e-2174g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4954
xeon_e-2146g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4955
xeon_e-2144g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable	N/A	H-INT-XEON-060820/4956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure via local access. **CVE ID : CVE-2020-0543**		
xeon_e-2136					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4957
xeon_e-2134					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4958
xeon_e-2126g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4959
xeon_e-2124					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R)	N/A	H-INT-XEON-060820/4960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
xeon_e-2124g					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-XEON-060820/4961
core_i7-7700					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-06-2020	4.6	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2020-0528**	N/A	H-INT-CORE-060820/4962
Improper Initialization	15-06-2020	4.6	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2020-0529**	N/A	H-INT-CORE-060820/4963
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read	N/A	H-INT-CORE-060820/4964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
ssd_dc_p4618					
Information Exposure	15-06-2020	2.1	Insufficient control flow management in firmware for some Intel(R) Data Center SSDs may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0527**	N/A	H-INT-SSD_-060820/4965
ssd_dc_p4511					
Information Exposure	15-06-2020	2.1	Insufficient control flow management in firmware for some Intel(R) Data Center SSDs may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0527**	N/A	H-INT-SSD_-060820/4966
celeron_3755u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CELE-060820/4967
core_4410y					
Information	15-06-2020	2.1	Incomplete cleanup from	N/A	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		060820/4968
core_4415y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4969
core_i3-i3-8100h					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4970
core_i5-7y57_					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-3840qm_					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-CORE-060820/4972
pentium_g3420					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4973
pentium_g4400					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4974
pentium_4405u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via	N/A	H-INT-PENT-060820/4975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-0543**		
pentium_4405y					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4976
pentium_3825u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4977
pentium_3805u					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**	N/A	H-INT-PENT-060820/4978
pentium_3560m					
Information Exposure	15-06-2020	2.1	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an	N/A	H-INT-PENT-060820/4979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2020-0543**		
Lenovo					
xiaoxin_air-14iwl_2019					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XIAO-060820/4980
xiaoxin_air-15iwl_2019					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XIAO-060820/4981
xiaoxin-14_2019iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XIAO-060820/4982
xiaoxin-14iwl_qc_2019					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XIAO-060820/4983
xiaoxin-15_2019iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XIAO-060820/4984
y7000_2019_1050					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-Y700-060820/4985
yoga_730-13iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	H-LEN-YOGA-060820/4986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
yoga_730-15iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-YOGA-060820/4987
yoga_s730-13iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-YOGA-060820/4988
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-YOGA-060820/4989
yoga_s940-14iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-YOGA-060820/4990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-YOGA-060820/4991
flex_6-1470					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-FLEX-060820/4992
zhaoyang_k42-80					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-ZHAO-060820/4993
l340-15irh					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-L340-060820/4994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
l340-17irh					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-L340-060820/4995
l340-17iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-L340-060820/4996
legion_y530-15ich					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/4997
legion_y730-15ich					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code	N/A	H-LEN-LEGI-060820/4998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-8321**		
legion_y7000p-1060					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/4999
legion_y730-17ich					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5000
legion_y740-15irhg					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5001
legion_y740-15ichg					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in	N/A	H-LEN-LEGI-060820/5002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
legion_y9000k_2019					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5003
legion_y740-17ichg					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5004
legion_y740-17irhg					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5005
legion_y9000p_2019					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	H-LEN-LEGI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		060820/5006
lenovo_v720-14ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LENO-060820/5007
330-14ikbr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330--060820/5008
330-15ikbr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330--060820/5009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
330-15ikbr_touch					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330--060820/5010
330-17ikbr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330--060820/5011
720s_touch-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-720S-060820/5012
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-720S-060820/5013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
720s-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-720S-060820/5014
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-720S-060820/5015
e53-80					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-E53--060820/5016
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-E53--060820/5017
k43c-80					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	H-LEN-K43C-060820/5018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
v330-14isk					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-V330-060820/5019
v330-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V330-060820/5020
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V330-060820/5021
v330-15isk					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo	N/A	H-LEN-V330-060820/5022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V330-060820/5023
v730-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V730-060820/5024
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V730-060820/5025
yoga_720-12ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	H-LEN-YOGA-060820/5026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
yoga_730-13ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-YOGA-060820/5027
yoga_730-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-YOGA-060820/5028
yoga_c930-13ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-YOGA-060820/5029
thinkpad_11e					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege.	N/A	H-LEN-THIN-060820/5030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8320		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5031
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5032
miix_720-12ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-MIIX-060820/5033
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-MIIX-060820/5034
rescuer_y7000p					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-RESC-060820/5035
rescuer_y7000p\(1060\)					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-RESC-060820/5036
rescuer_y7000					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-RESC-060820/5037
rescuer_y7000\(1060\)					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	H-LEN-RESC-060820/5038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
s145-14iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S145-060820/5039
s145-14ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S145-060820/5040
s145-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S145-060820/5041
s145-15iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may	N/A	H-LEN-S145-060820/5042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
340c-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-340C-060820/5043
s340-14iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S340-060820/5044
s340-14iwl_touch					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S340-060820/5045
s340-15iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	H-LEN-S340-060820/5046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
s340-15iwl_touch					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S340-060820/5047
s530-13iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S530-060820/5048
s540-14iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S540-060820/5049
Unquoted Search Path	09-06-2020	7.2	An unquoted search path vulnerability was reported	N/A	H-LEN-S540-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
or Element			in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**		060820/5050
s540-14iwl_touch					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S540-060820/5051
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-S540-060820/5052
s540-15iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S540-060820/5053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
s940-14iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-S940-060820/5054
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-S940-060820/5055
v110-14ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V110-060820/5056
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V110-060820/5057
v130-14ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	H-LEN-V130-060820/5058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
v130-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V130-060820/5059
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V130-060820/5060
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-V130-060820/5061
v320-14ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in	N/A	H-LEN-V320-060820/5062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
v320-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-V320-060820/5063
v320-17ikbr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-V320-060820/5064
wei5-14ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-WEI5-060820/5065
wei5-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	H-LEN-WEI5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		060820/5066
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-WEI5-060820/5067
xiaoxin_air_13iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XIAO-060820/5068
xiaoxin_air_14ikbr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XIAO-060820/5069
xiaoxin_air_14iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function	N/A	H-LEN-XIAO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		060820/5070
xiaoxin_air_15ikbr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XIAO-060820/5071
xiaoxin_air_15iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XIAO-060820/5072
thinkpad_e450					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_e450c					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5074
thinkpad_e550					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5075
thinkpad_e550c					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5076
thinkpad_e490s					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of	N/A	H-LEN-THIN-060820/5077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5078
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5079
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5080
thinkpad_s3					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5081
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad,	N/A	H-LEN-THIN-060820/5082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5083
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5084
thinkpad_11e_yoga_gen_6					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5085
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5086
thinkpad_yoga_11e_3rd_gen					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5087
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5088
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5089
thinkpad_yoga_11e_4th_gen					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5090
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	N/A	H-LEN-THIN-060820/5091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8323		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5092
thinkpad_yoga_11e_5th_gen					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5093
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5094
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5095
thinkpad_13_2nd_gen					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5096
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5097
thinkpad_e455					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5098
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5099
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code.	N/A	H-LEN-THIN-060820/5100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8337		
thinkpad_e555					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5101
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5102
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5103
legion_y7000_pg0					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5104
legion_y7000p_2019					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5105
legion_y7000p_pg0					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5106
lenovo_e41-25					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LENO-060820/5107
lenovo_v320-17ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	H-LEN-LENO-060820/5108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
s145-14					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S145-060820/5109
s145-14igm					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S145-060820/5110
s145-15igm					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S145-060820/5111
s340-13iml					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may	N/A	H-LEN-S340-060820/5112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
s340-14					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S340-060820/5113
s340-14api					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S340-060820/5114
s340-14iil					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S340-060820/5115
s340-14iml					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	H-LEN-S340-060820/5116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
s340-15api					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S340-060820/5117
s340-15iml					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S340-060820/5118
s530-13iml					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S530-060820/5119
s540-14api					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S540-060820/5120
s540-14iml					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S540-060820/5121
s540-15iml					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S540-060820/5122
s540-15iwl_gtx					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	H-LEN-S540-060820/5123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
s550-14iil					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-S550-060820/5124
v130-14ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-V130-060820/5125
v130-14igm					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-V130-060820/5126
v130-15ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may	N/A	H-LEN-V130-060820/5127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
v145-14ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-V145-060820/5128
v145-15ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-V145-060820/5129
v330-14arr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-V330-060820/5130
v330-14ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	H-LEN-V330-060820/5131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
v330-14igm					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-V330-060820/5132
v330-15ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-V330-060820/5133
xiaoxin_air_14arr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XIAO-060820/5134
xiaoxin-13iml					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XIAO-060820/5135
xiaoxin-14igm_qc_2019					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XIAO-060820/5136
xx-14kb_qc_2019					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-XX-1-060820/5137
yoga_530-14arr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	H-LEN-YOGA-060820/5138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8321		
yoga_c740-14iml					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-YOGA-060820/5139
yoga_c740-15iml					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-YOGA-060820/5140
yoga_c930_glass					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-YOGA-060820/5141
yoga_c940					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may	N/A	H-LEN-YOGA-060820/5142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
yoga_s740-14iil					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-YOGA-060820/5143
yoga_530-14ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-YOGA-060820/5144
e43-80_kbl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-E43--060820/5145
thinkpad_s1_yoga_vpro					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	H-LEN-THIN-060820/5146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_t540					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5147
thinkpad_x1_carbon_\(20ax\)					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5148
thinkpad_x1_carbon_\(20bx\)					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5149
thinkpad_yoga_11e_\(20dx\)					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad,	N/A	H-LEN-THIN-060820/5150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkagile_2u4n_certified_node					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5151
thinkagile_hx1320					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5152
thinkagile_hx1321					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5153
thinkagile_hx1520-r					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of	N/A	H-LEN-THIN-060820/5154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		
thinkagile_hx1521-r					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5155
thinkagile_hx2320					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5156
thinkagile_hx2320-e					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkagile_hx2520-r					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5158
thinkagile_hx2521-r					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5159
thinkagile_hx2710e					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5160
thinkagile_vx5520					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to	N/A	H-LEN-THIN-060820/5161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system memory. **CVE ID : CVE-2020-8331**		
thinkagile_vx7320-n					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5162
thinkagile_vx7520					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5163
thinkagile_vx7520-n					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5164
thinksystem_sr650_expansion					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA	N/A	H-LEN-THIN-060820/5165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		
vx_2u_certified_node					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-VX_2-060820/5166
thinksystem_dn8836					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5167
thinksystem_se350					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5168
thinksystem_sr635					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	H-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		060820/5169
thinksystem_st50					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5170
thinkpad_l13_1st_gen					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5171
thinkpad_l1415_gen_1					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5172
thinkpad_p1_\(20mx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB	N/A	H-LEN-THIN-060820/5173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**		
thinkpad_p1_\(20qx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5174
thinkpad_p52_\(20mx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5175
thinkpad_p53_\(20qx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5176
thinkpad_l1415					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5178
thinkpad_s5_2nd_gen					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5179
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5180
thinkpad_s1					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5181
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	N/A	H-LEN-THIN-060820/5182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8323		
thinkpad_t495s					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5183
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5184
Incorrect Authorizatio n	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	H-LEN-THIN-060820/5185
330-14ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-330--060820/5186
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo	N/A	H-LEN-330--060820/5187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
330-15ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-330--060820/5188
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-330--060820/5189
330-17ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-330--060820/5190
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-330--060820/5191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
340c-15api					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-340C-060820/5192
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-340C-060820/5193
340c-15ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-340C-060820/5194
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-340C-060820/5195
c640-iml					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB	N/A	H-LEN-C640-060820/5196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-C640-060820/5197
k22-80					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-K22--060820/5198
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-K22--060820/5199
v720-12					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	H-LEN-V720-060820/5200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8322		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V720-060820/5201
k32-80_kbl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-K32--060820/5202
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-K32--060820/5203
k32-80_skl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-K32--060820/5204
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	H-LEN-K32--060820/5205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
s145-14api					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-S145-060820/5206
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-S145-060820/5207
s145-14ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-S145-060820/5208
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	N/A	H-LEN-S145-060820/5209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8323		
s145-15api					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-S145-060820/5210
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-S145-060820/5211
s145-15ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-S145-060820/5212
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-S145-060820/5213
s540-13api					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	H-LEN-S540-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		060820/5214
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-S540-060820/5215
s750-iil					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-S750-060820/5216
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-S750-060820/5217
thinkbook_13s-iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation	N/A	H-LEN-THIN-060820/5218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5219
thinkbook_14s-iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-THIN-060820/5220
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5221
v110-14ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V110-060820/5222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V110-060820/5223
v110-15ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V110-060820/5224
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V110-060820/5225
v130-15igm					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V130-060820/5226
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad,	N/A	H-LEN-V130-060820/5227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-V130-060820/5228
v310-15igm					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V310-060820/5229
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V310-060820/5230
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could	N/A	H-LEN-V310-060820/5231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**		
v340-iil					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V340-060820/5232
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V340-060820/5233
v340-iml					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V340-060820/5234
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V340-060820/5235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
v540s-13					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V540-060820/5236
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V540-060820/5237
14iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-14IW-060820/5238
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-14IW-060820/5239
v730-13ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB	N/A	H-LEN-V730-060820/5240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V730-060820/5241
v730-13isk					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V730-060820/5242
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V730-060820/5243
xiaoxin_14-ast_qc_2019					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution.	N/A	H-LEN-XIAO-060820/5244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8322		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-XIAO-060820/5245
xx-14api_qc_2019					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-XX-1-060820/5246
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-XX-1-060820/5247
6_pro-13-iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-6_PR-060820/5248
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	H-LEN-6_PR-060820/5249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
6_pro-14-iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-6_PR-060820/5250
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-6_PR-060820/5251
k3					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-K3-060820/5252
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	N/A	H-LEN-K3-060820/5253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8323		
k4-iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-K4-I-060820/5254
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-K4-I-060820/5255
5-15ikb					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-5-15-060820/5256
air-14_2019					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user	N/A	H-LEN-AIR--060820/5257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary code. **CVE ID : CVE-2020-8337**		
thinkpad_e540					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5258
thinkpad_e545					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5259
thinkpad_edge_e440					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5260
thinkpad_edge_e445					
Unquoted	09-06-2020	7.2	An unquoted search path	N/A	H-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Search Path or Element			vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**		060820/5261
thinkpad_l440					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5262
thinkpad_l540					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5263
thinkpad_s1_yoga_12					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on	N/A	H-LEN-THIN-060820/5264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**		
thinkpad_yoga_14_460_s3					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5265
130-14ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-130--060820/5266
130-15ast					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-130--060820/5267
320c-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	H-LEN-320C-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		060820/5268
330-15arr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330--060820/5269
330-15arr_touch					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330--060820/5270
340c-15igm					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-340C-060820/5271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
530s-14arr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-530S-060820/5272
thinkpad_13					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5273
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5274
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5275
thinkpad_a275					
Improper Privilege	09-06-2020	4.6	An internal shell was included in BIOS image in	N/A	H-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**		060820/5276
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5277
Incorrect Authorizatio n	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	H-LEN-THIN-060820/5278
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5279
thinkpad_a475					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5281
Incorrect Authorization	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	H-LEN-THIN-060820/5282
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5283
thinkpad_e460					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5284
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo	N/A	H-LEN-THIN-060820/5285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5286
thinkpad_e560					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5287
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5288
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_e465					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5290
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5291
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5292
thinkpad_e565					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5293
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow	N/A	H-LEN-THIN-060820/5294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-8323**		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5295
thinkpad_e470					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5296
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5297
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_e570					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5299
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5300
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5301
thinkpad_e475					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5302
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow	N/A	H-LEN-THIN-060820/5303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-8323**		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5304
thinkpad_e575					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5305
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5306
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_e480					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5308
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5309
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5310
thinkpad_e580					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5311
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow	N/A	H-LEN-THIN-060820/5312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-8323**		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5313
thinkpad_e485					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5314
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5315
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_e585					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5317
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5318
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5319
thinkpad_s5					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5320
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow	N/A	H-LEN-THIN-060820/5321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-8323**		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5322
thinkpad_l380					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5323
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5324
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_l380_yoga					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5326
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5327
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5328
thinkpad_l460					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5329
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow	N/A	H-LEN-THIN-060820/5330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-8323**		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5331
thinkpad_l470					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5332
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5333
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_l480					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5335
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5336
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5337
thinkpad_l580					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5338
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow	N/A	H-LEN-THIN-060820/5339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-8323**		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5340
thinkpad_l560					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5341
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5342
thinkpad_l570					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5343
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	H-LEN-THIN-060820/5344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_p40					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5345
thinkpad_p50					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5346
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5347
thinkpad_p50s					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege.	N/A	H-LEN-THIN-060820/5348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8320		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5349
thinkpad_p51s					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5350
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5351
thinkagile_hx2720-e					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5352
thinkagile_hx3320					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of	N/A	H-LEN-THIN-060820/5353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		
thinkagile_hx3321					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5354
thinkagile_hx3520-g					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5355
thinkagile_hx3521-g					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkagile_hx3710					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5357
thinkagile_hx3720					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5358
thinkagile_hx3721					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5359
thinkagile_hx3731					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to	N/A	H-LEN-THIN-060820/5360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system memory. **CVE ID : CVE-2020-8331**		
thinkagile_hx5520					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5361
thinkagile_hx5520-c					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5362
thinkagile_hx5521					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5363
thinkagile_hx5521-c					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA	N/A	H-LEN-THIN-060820/5364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		
thinkagile_hx7520					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5365
thinkagile_hx7521					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5366
thinkagile_hx7820					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5367
thinkagile_hx7821					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	H-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		060820/5368
thinkagile_mx_certified_node_all_flash					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5369
thinkagile_mx_certified_node_entry					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5370
thinkagile_mx_certified_node_hybrid					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkagile_vx_1se_certified_node					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5372
thinkagile_vx_1u_certified_node					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5373
thinkagile_vx_2u_certified_node					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5374
thinkagile_vx1320					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to	N/A	H-LEN-THIN-060820/5375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system memory. **CVE ID : CVE-2020-8331**		
thinkagile_vx2320					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5376
thinkagile_vx3320					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5377
thinkagile_vx3520-g					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5378
thinkagile_vx3720					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA	N/A	H-LEN-THIN-060820/5379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		
130-14ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-130--060820/5380
130-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-130--060820/5381
330-14ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330--060820/5382
330-15ich					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	H-LEN-330--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		060820/5383
330-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330--060820/5384
330-17ich					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330--060820/5385
330-17ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330--060820/5386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
330c-14ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330C-060820/5387
330c-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330C-060820/5388
330c-15ikbr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330C-060820/5389
340c-15iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code	N/A	H-LEN-340C-060820/5390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-8321**		
530s-14iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-530S-060820/5391
530s-15iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-530S-060820/5392
530s-14ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-530S-060820/5393
530s-15ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in	N/A	H-LEN-530S-060820/5394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
720s-14ikbr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-720S-060820/5395
730s-13iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-730S-060820/5396
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-730S-060820/5397
c340-14iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and	N/A	H-LEN-C340-060820/5398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-C340-060820/5399
c340-15iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-C340-060820/5400
e42-80					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-E42--060820/5401
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo	N/A	H-LEN-E42--060820/5402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
e52-80					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-E52--060820/5403
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-E52--060820/5404
flex_6-14ikb					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-FLEX-060820/5405
flex-14iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code	N/A	H-LEN-FLEX-060820/5406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-8321**		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-FLEX-060820/5407
flex-15iwl					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-FLEX-060820/5408
thinkpad_p52s					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5409
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_p70					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5411
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5412
thinkpad_s3_yoga_14					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5413
thinkpad_s3-s440					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_e560p					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5415
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5416
thinkpad_t25					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5417
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5418
thinkpad_t460					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5420
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5421
thinkpad_t460p					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5422
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5423
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the	N/A	H-LEN-THIN-060820/5424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**		
thinkpad_t460s					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5425
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5426
thinkpad_t470					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5427
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5428
thinkpad_t470p					
Improper	09-06-2020	4.6	An internal shell was	N/A	H-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**		060820/5429
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5430
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5431
thinkpad_t470s					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5432
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_t480					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5434
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5435
thinkpad_t480s					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5436
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5437
thinkpad_t560					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5439
thinkpad_t570					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5440
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5441
thinkpad_t580					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5442
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	N/A	H-LEN-THIN-060820/5443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8323		
thinkpad_x1_carbon					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5444
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5445
thinkpad_x1_yoga					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5446
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5447
thinkpad_x1_tablet					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege.	N/A	H-LEN-THIN-060820/5448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8320		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5449
thinkpad_x260					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5450
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5451
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5452
thinkpad_x270					
Improper Privilege	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that	N/A	H-LEN-THIN-060820/5453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			could allow escalation of privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5454
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5455
thinkpad_x280					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5456
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5457
thinkpad_x380_yoga					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5458
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5459
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5460
thinkpad_yoga_260					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5461
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	N/A	H-LEN-THIN-060820/5462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8323		
330-14igm					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330--060820/5463
330-15igm					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-330--060820/5464
thinkstation_p410					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-THIN-060820/5465
thinkstation_p500					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may	N/A	H-LEN-THIN-060820/5466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
thinkstation_p510					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-THIN-060820/5467
thinkstation_p520					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-THIN-060820/5468
thinkstation_p520c					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-THIN-060820/5469
thinkstation_p700					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock	N/A	H-LEN-THIN-060820/5470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
thinkstation_p710					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-THIN-060820/5471
thinkstation_p720					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-THIN-060820/5472
thinkstation_p900					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-THIN-060820/5473
thinkstation_p910					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-THIN-060820/5474
thinkstation_p920					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-THIN-060820/5475
thinksystem_sd530					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5476
thinksystem_sd650					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory.	N/A	H-LEN-THIN-060820/5477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8331		
thinksystem_sn550					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5478
thinksystem_sn850					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5479
thinksystem_sr150					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5480
thinksystem_sr250					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access	N/A	H-LEN-THIN-060820/5481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read or write access to system memory. **CVE ID : CVE-2020-8331**		
thinksystem_sr258					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5482
thinksystem_sr850					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5483
thinksystem_sr860					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5484
thinksystem_st250					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models	N/A	H-LEN-THIN-060820/5485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**		
thinksystem_sr530					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5486
thinksystem_sr550					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5487
thinksystem_sr570					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5488
thinksystem_sr590					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5489
thinksystem_sr630					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5490
thinksystem_sr650					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5491
thinksystem_st550					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory.	N/A	H-LEN-THIN-060820/5492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8331		
thinksystem_st558					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5493
thinksystem_sr950					
N/A	09-06-2020	4.6	A potential vulnerability in the BIOS configuration of some ThinkSystem models due to missing DMA protections that may allow a user with physical access read or write access to system memory. **CVE ID : CVE-2020-8331**	N/A	H-LEN-THIN-060820/5494
thinkpad_t440p					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5495
thinkpad_t450					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could	N/A	H-LEN-THIN-060820/5496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**		
thinkpad_t450s					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5497
thinkpad_t490					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5498
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5499
thinkpad_t490s					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5500
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	H-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		060820/5501
thinkpad_t540p					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5502
thinkpad_t550					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5503
thinkpad_t590					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5504
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow	N/A	H-LEN-THIN-060820/5505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_w540					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5506
thinkpad_w541					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5507
thinkpad_w550s					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5508
thinkpad_x1_extreme					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5510
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5511
thinkpad_x140e					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5512
thinkpad_x240					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5513
thinkpad_x240s					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5514
thinkpad_x250					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5515
thinkpad_x390					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5516
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5517
thinkpad_x390_yoga					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of	N/A	H-LEN-THIN-060820/5518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege. **CVE ID : CVE-2020-8320**		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5519
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5520
thinkpad_yoga_11e					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5521
thinkpad_yoga_370					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5522
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function	N/A	H-LEN-THIN-060820/5523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5524
thinkpad_s1_3rd					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5525
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5526
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could	N/A	H-LEN-THIN-060820/5527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**		
yoga_14					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-YOGA-060820/5528
thinkpad_a285					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5529
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5530
Incorrect Authorization	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	H-LEN-THIN-060820/5531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5532
thinkpad_a485					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5533
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5534
Incorrect Authorizatio n	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	H-LEN-THIN-060820/5535
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the	N/A	H-LEN-THIN-060820/5536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**		
thinkpad_e14					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5537
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5538
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5539
thinkpad_e15					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5540
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	H-LEN-THIN-060820/5541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5542
thinkpad_l13					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5543
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5544
thinkpad_p43s					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5545
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	H-LEN-THIN-060820/5546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_r14					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5547
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5548
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5549
thinkpad_s3_gen_2					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5550
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	H-LEN-THIN-060820/5551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5552
thinkpad_t495					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5553
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5554
Incorrect Authorization	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	H-LEN-THIN-060820/5555
thinkpad_x395					
Improper	09-06-2020	4.6	An internal shell was	N/A	H-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**		060820/5556
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5557
Incorrect Authorization	09-06-2020	4.6	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad T495s, X395, T495, A485, A285, A475, A275 which may allow for unauthorized access. **CVE ID : CVE-2020-8334**	N/A	H-LEN-THIN-060820/5558
v330-15igm					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy USB driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8322**	N/A	H-LEN-V330-060820/5559
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-V330-060820/5560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-V330-060820/5561
thinkpad_p53s_\(20nx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5562
thinkpad_p72_\(20mx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5563
thinkpad_p73_\(20qx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5564
thinkpad_t490_\(20nx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB	N/A	H-LEN-THIN-060820/5565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**		
thinkpad_t490_\(20qx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5566
thinkpad_t490_\(20rx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5567
thinkpad_t490s_\(20nx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5568
thinkpad_t590_\(20nx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_x1_carbon_\(20qx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5570
thinkpad_x1_carbon_\(20rx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5571
thinkpad_x1_extreme_\(20mx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5572
thinkpad_x1_extreme_\(20qx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5573
thinkpad_x1_yoga_\(20qx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent	N/A	H-LEN-THIN-060820/5574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**		
thinkpad_x1_yoga_\(20sx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5575
thinkpad_x390_\(20qx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5576
thinkpad_x390_\(20sx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5577
thinkpad_e490					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5578
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver	N/A	H-LEN-THIN-060820/5579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5580
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5581
thinkpad_e590					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5582
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5584
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5585
thinkpad_r490					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5586
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5587
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash.	N/A	H-LEN-THIN-060820/5588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8336		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5589
thinkpad_r590					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5590
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5591
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5592
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the	N/A	H-LEN-THIN-060820/5593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**		
thinkpad_helix					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5594
thinkpad_s3_3rd_gen					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5595
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5596
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code.	N/A	H-LEN-THIN-060820/5597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8337		
thinkpad_s2_yoga_3rd_gen					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5598
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5599
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5600
thinkpad_l390_yoga					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5601
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo	N/A	H-LEN-THIN-060820/5602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5603
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5604
thinkpad_s2_yoga_4th_gen					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5605
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5606
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some	N/A	H-LEN-THIN-060820/5607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**		
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5608
thinkpad_l450					
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5609
thinkpad_l490					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5610
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow	N/A	H-LEN-THIN-060820/5611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-8323**		
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5612
thinkpad_l590					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5613
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5614
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5615
thinkpad_p1					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege.	N/A	H-LEN-THIN-060820/5616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8320		
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5617
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**	N/A	H-LEN-THIN-060820/5618
thinkpad_p43s_\(20rx\)					
N/A	09-06-2020	4.6	Lenovo implemented Intel CSME Anti-rollback ARB protections on some ThinkPad models to prevent roll back of CSME Firmware in flash. **CVE ID : CVE-2020-8336**	N/A	H-LEN-THIN-060820/5619
thinkpad_p51					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5620
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad,	N/A	H-LEN-THIN-060820/5621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**		
thinkpad_p52					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5622
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5623
thinkpad_p53					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5624
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5625
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0	N/A	H-LEN-THIN-060820/5626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user to execute arbitrary code. **CVE ID : CVE-2020-8337**		
thinkpad_p53s					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5627
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5628
thinkpad_p71					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5629
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_p72					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5631
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5632
thinkpad_p73					
Improper Privilege Management	09-06-2020	4.6	An internal shell was included in BIOS image in some ThinkPad models that could allow escalation of privilege. **CVE ID : CVE-2020-8320**	N/A	H-LEN-THIN-060820/5633
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5634
Unquoted Search Path or Element	09-06-2020	7.2	An unquoted search path vulnerability was reported in versions prior to 1.0.83.0 of the Synaptics Smart Audio UWP app associated with the DCHU audio drivers on Lenovo platforms that could allow an administrative user	N/A	H-LEN-THIN-060820/5635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary code. **CVE ID : CVE-2020-8337**		
thinkpad_s1_yoga					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5636
thinkpad_s5_yoga_15					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5637
thinkpad_s540					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5638
thinkpad_t440					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution.	N/A	H-LEN-THIN-060820/5639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8323		
thinkpad_t440s					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the Legacy SD driver in some Lenovo ThinkPad, ThinkStation, and Lenovo Notebook models may allow arbitrary code execution. **CVE ID : CVE-2020-8323**	N/A	H-LEN-THIN-060820/5640
720s-13arr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-720S-060820/5641
c340-14api					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-C340-060820/5642
c340-14iml					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code	N/A	H-LEN-C340-060820/5643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-8321**		
c340-15iil					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-C340-060820/5644
c340-15iml					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-C340-060820/5645
d330-10igm					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-D330-060820/5646
d335-10igm					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in	N/A	H-LEN-D335-060820/5647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
e4-14arr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-E4-1-060820/5648
flex_6-14arr					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-FLEX-060820/5649
ideapad_3_14					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-IDEA-060820/5650
ideapad_3_15					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	H-LEN-IDEA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		060820/5651
ideapad_3_17iml05					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-IDEA-060820/5652
ideapad_3_15iil05					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-IDEA-060820/5653
ideapad_3_14iil05					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-IDEA-060820/5654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ideapad_5_15iil05					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-IDEA-060820/5655
l3_15iml05					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-L3_1-060820/5656
l340-15api					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-L340-060820/5657
l340-15api_touch					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code	N/A	H-LEN-L340-060820/5658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-8321**		
l340-15iwl_touch					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-L340-060820/5659
l340-17api					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-L340-060820/5660
legion_y530-15ich-1060					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5661
legion_y540-15_pg0					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in	N/A	H-LEN-LEGI-060820/5662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		
legion_y540-15irh					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5663
legion_y540-17_pg0					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5664
legion_y540-17irh					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5665
legion_y545					
N/A	09-06-2020	4.6	A potential vulnerability in	N/A	H-LEN-LEGI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**		060820/5666
legion_y545_pg0					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5667
legion_y7000_2019					
N/A	09-06-2020	4.6	A potential vulnerability in the SMI callback function used in the System Lock Preinstallation driver in some Lenovo Notebook and ThinkStation models may allow arbitrary code execution. **CVE ID : CVE-2020-8321**	N/A	H-LEN-LEGI-060820/5668
LG					
cv1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007	https://lgsecurity.lge.com/	H-LG-CV1-060820/5669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(June 2020). **CVE ID : CVE-2020-13839**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-CV1-060820/5670
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-CV1-060820/5671
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-CV1-060820/5672
cv1s					
Buffer Copy without Checking Size of Input ('Classic	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a	https://lgsecurity.lge.com/	H-LG-CV1S-060820/5673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-CV1S-060820/5674
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-CV1S-060820/5675
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-CV1S-060820/5676
cv3					
Buffer Copy without	05-06-2020	10	An issue was discovered on LG mobile devices with	https://lgsecurity.lge.co	H-LG-CV3-060820/5677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	m/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-CV3-060820/5678
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-CV3-060820/5679
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-CV3-060820/5680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
cv5					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-CV5-060820/5681
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-CV5-060820/5682
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-CV5-060820/5683
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June	https://lgsecurity.lge.com/	H-LG-CV5-060820/5684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020). **CVE ID : CVE-2020-13842**		
cv7					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-CV7-060820/5685
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-CV7-060820/5686
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-CV7-060820/5687
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was	https://lgsecurity.lge.com/	H-LG-CV7-060820/5688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**		
cv7as					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-CV7A-060820/5689
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-CV7A-060820/5690
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-CV7A-060820/5691
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with	https://lgsecurity.lge.co	H-LG-CV7A-060820/5692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	m/	
dh10					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-DH10-060820/5693
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-DH10-060820/5694
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020).	https://lgsecurity.lge.com/	H-LG-DH10-060820/5695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13841		
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-DH10-060820/5696
dh15					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-DH15-060820/5697
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-DH15-060820/5698
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is	https://lgsecurity.lge.com/	H-LG-DH15-060820/5699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**		
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-DH15-060820/5700
dh30					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-DH30-060820/5701
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-DH30-060820/5702
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command	https://lgsecurity.lge.com/	H-LG-DH30-060820/5703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**		
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-DH30-060820/5704
dh35					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-DH35-060820/5705
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-DH35-060820/5706
Improper	05-06-2020	10	An issue was discovered on	https://lgse	H-LG-DH35-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	curity.lge.com/	060820/5707
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-DH35-060820/5708
dh40					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-DH40-060820/5709
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020).	https://lgsecurity.lge.com/	H-LG-DH40-060820/5710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13840		
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-DH40-060820/5711
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-DH40-060820/5712
dh5					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-DH5-060820/5713
Buffer Copy without Checking Size of Input ('Classic Buffer	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is	https://lgsecurity.lge.com/	H-LG-DH5-060820/5714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**		
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-DH5-060820/5715
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-DH5-060820/5716
dh50					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-DH50-060820/5717
Buffer Copy without Checking Size of Input	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code	https://lgsecurity.lge.com/	H-LG-DH50-060820/5718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**		
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-DH50-060820/5719
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-DH50-060820/5720
g6					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-G6-060820/5721
Buffer Copy	05-06-2020	7.5	An issue was discovered on	https://lgse	H-LG-G6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	curity.lge.com/	060820/5722
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-G6-060820/5723
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-G6-060820/5724
g7					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020).	https://lgsecurity.lge.com/	H-LG-G7-060820/5725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13839		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-G7-060820/5726
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-G7-060820/5727
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-G7-060820/5728
g8					
Buffer Copy without Checking Size of Input ('Classic Buffer	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The	https://lgsecurity.lge.com/	H-LG-G8-060820/5729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-G8-060820/5730
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-G8-060820/5731
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-G8-060820/5732
k20					
Buffer Copy without Checking Size of Input	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code	https://lgsecurity.lge.com/	H-LG-K20-060820/5733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-K20-060820/5734
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-K20-060820/5735
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-K20-060820/5736
k30					
Buffer Copy	05-06-2020	10	An issue was discovered on	https://lgse	H-LG-K30-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	curity.lge.com/	060820/5737
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-K30-060820/5738
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-K30-060820/5739
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-K30-060820/5740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
k40					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-K40-060820/5741
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-K40-060820/5742
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-K40-060820/5743
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June	https://lgsecurity.lge.com/	H-LG-K40-060820/5744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020). **CVE ID : CVE-2020-13842**		
k50					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-K50-060820/5745
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-K50-060820/5746
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-K50-060820/5747
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was	https://lgsecurity.lge.com/	H-LG-K50-060820/5748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**		
q6					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-Q6-060820/5749
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-Q6-060820/5750
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-Q6-060820/5751
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with	https://lgsecurity.lge.co	H-LG-Q6-060820/5752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	m/	
q60					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-Q60-060820/5753
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-Q60-060820/5754
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020).	https://lgsecurity.lge.com/	H-LG-Q60-060820/5755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13841		
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-Q60-060820/5756
q70					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-Q70-060820/5757
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-Q70-060820/5758
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is	https://lgsecurity.lge.com/	H-LG-Q70-060820/5759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**		
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-Q70-060820/5760
q8					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-Q8-060820/5761
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-Q8-060820/5762
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command	https://lgsecurity.lge.com/	H-LG-Q8-060820/5763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**		
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-Q8-060820/5764
v20					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-V20-060820/5765
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-V20-060820/5766
Improper	05-06-2020	10	An issue was discovered on	https://lgse	H-LG-V20-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	curity.lge.com/	060820/5767
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-V20-060820/5768
v30					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-V30-060820/5769
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020).	https://lgsecurity.lge.com/	H-LG-V30-060820/5770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13840		
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-V30-060820/5771
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-V30-060820/5772
v35					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-V35-060820/5773
Buffer Copy without Checking Size of Input ('Classic Buffer	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is	https://lgsecurity.lge.com/	H-LG-V35-060820/5774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**		
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-V35-060820/5775
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-V35-060820/5776
v40					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-V40-060820/5777
Buffer Copy without Checking Size of Input	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code	https://lgsecurity.lge.com/	H-LG-V40-060820/5778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**		
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-V40-060820/5779
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-V40-060820/5780
v50					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-V50-060820/5781
Buffer Copy	05-06-2020	7.5	An issue was discovered on	https://lgse	H-LG-V50-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	curity.lge.com/	060820/5782
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-V50-060820/5783
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-V50-060820/5784
v60					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020).	https://lgsecurity.lge.com/	H-LG-V60-060820/5785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13839		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-V60-060820/5786
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-V60-060820/5787
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-V60-060820/5788
x300					
Buffer Copy without Checking Size of Input ('Classic Buffer	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The	https://lgsecurity.lge.com/	H-LG-X300-060820/5789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-X300-060820/5790
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-X300-060820/5791
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-X300-060820/5792
x400					
Buffer Copy without Checking Size of Input	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code	https://lgsecurity.lge.com/	H-LG-X400-060820/5793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-X400-060820/5794
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-X400-060820/5795
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-X400-060820/5796
x500					
Buffer Copy	05-06-2020	10	An issue was discovered on	https://lgse	H-LG-X500-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	curity.lge.com/	060820/5797
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-X500-060820/5798
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-X500-060820/5799
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020). **CVE ID : CVE-2020-13842**	https://lgsecurity.lge.com/	H-LG-X500-060820/5800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
x_cam					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020). **CVE ID : CVE-2020-13839**	https://lgsecurity.lge.com/	H-LG-X_CA-060820/5801
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-06-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020). **CVE ID : CVE-2020-13840**	https://lgsecurity.lge.com/	H-LG-X_CA-060820/5802
Improper Privilege Management	05-06-2020	10	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020). **CVE ID : CVE-2020-13841**	https://lgsecurity.lge.com/	H-LG-X_CA-060820/5803
N/A	05-06-2020	4.6	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June	https://lgsecurity.lge.com/	H-LG-X_CA-060820/5804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020). **CVE ID : CVE-2020-13842**		
Mitsubishielectric					
melsec_iq-r08cpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5805
melsec_iq-r16cpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5806
melsec_iq-r32cpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/202	H-MIT-MELS-060820/5807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	0-001_en.pdf	
melsec_iq-r120cpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5808
melsec_iq-r08fcpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5809
melsec_iq-r16fcpu					
Uncontrolled Resource	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware	https://www.mitsubish	H-MIT-MELS-060820/5810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	ielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	
melsec_iq-r32fcpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5811
melsec_iq-r120fcpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
melsec_iq-r08pcpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5813
melsec_iq-r16pcpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5814
melsec_iq-r32pcpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**		
melsec_iq-r120pcpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5816
melsec_iq-r08sfcpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5817
melsec_iq-r16sfcpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/202	H-MIT-MELS-060820/5818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	0-001_en.pdf	
melsec_iq-r32sfcpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5819
melsec_iq-r120sfcpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5820
melsec_iq-rj71en71					
Uncontrolled Resource	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware	https://www.mitsubish	H-MIT-MELS-060820/5821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	ielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	
melsec_iq-r00cpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5822
melsec_iq-r01cpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
melsec_iq-r02cpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5824
melsec_iq-r04cpu					
Uncontrolled Resource Consumption	10-06-2020	7.8	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production. **CVE ID : CVE-2020-13238**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-001_en.pdf	H-MIT-MELS-060820/5825
NEC					
wr8165n					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription	N/A	H-NEC-WR81-060820/5826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
Netgear					
wnhde111					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-NET-WNHD-060820/5827
Qualcomm					
mdm9206					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5829
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5832
mdm9607					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5833
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5836
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
msm8909w					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5839
Improper Restriction of Operations within the Bounds of a	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MSM8-060820/5840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	lletins/may-2020-bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3641		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5843
msm8996au					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5845
Buffer Copy without	02-06-2020	7.2	Buffer overflow in display function due to memory	https://www.qualcom	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	m.com/company/product-security/bulletins/may-2020-bulletin	060820/5846
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3633		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5849
qca6574au					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCA6-060820/5850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCA6-060820/5851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
qcs405					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCS4-060820/5852
Improper Restriction of Operations	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon	https://www.qualcomm.com/company/produ	H-QUA-QCS4-060820/5853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	ct-security/bulletins/may-2020-bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCS4-060820/5854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCS4-060820/5855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCS4-060820/5856
qcs605					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCS6-060820/5857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCS6-060820/5858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCS6-060820/5859
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCS6-060820/5860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCS6-060820/5861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCS6-060820/5862
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more	https://www.qualcomm.com/company/produ	H-QUA-QCS6-060820/5863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	ct-security/bulletins/may-2020-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCS6-060820/5864
sda660					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDA6-060820/5865
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDA6-060820/5866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDA6-060820/5867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDA6-060820/5868
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may	H-QUA-SDA6-060820/5869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	-2020-bulletin	
sdm439					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/5870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/5871
Improper Restriction of	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video	https://www.qualcomm.com/com	H-QUA-SDM4-060820/5872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	pany/product-security/bulletins/may-2020-bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/5873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/5874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/5875
sdm630					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5878
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5881
sdm660					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-SDM6-060820/5882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	bulletin	
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5884
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-SDM6-060820/5885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5887
sdx20					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDX2-060820/5888
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDX2-060820/5889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDX2-060820/5890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3616		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDX2-060820/5891
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may	H-QUA-SDX2-060820/5892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	-2020-bulletin	
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDX2-060820/5893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
mdm9150					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5894
Improper Restriction of Operations	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon	https://www.qualcomm.com/company/produ	H-QUA-MDM9-060820/5895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	ct-security/bulletins/may-2020-bulletin	
mdm9640					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
mdm9650					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3630		
sdx24					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDX2-060820/5899
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check	https://www.qualcomm.com/company/product-security/bulletins/may	H-QUA-SDX2-060820/5900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDX2-060820/5901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDX2-060820/5902
ipq8074					
Use After Free	02-06-2020	7.2	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-IPQ8-060820/5903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SXR2130 **CVE ID : CVE-2020-3618**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-IPQ8-060820/5904
qca6174a					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCA6-060820/5905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
qca9377					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCA9-060820/5906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
qca9379					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCA9-060820/5907
sdm429w					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/may	H-QUA-SDM4-060820/5908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/5909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/5910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/5911
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/5912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**		
sc7180					
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SC71-060820/5913
apq8009					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL	https://www.qualcomm.com/company/produ	H-QUA-APQ8-060820/5914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	ct-security/bulletins/may-2020-bulletin	
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5917
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-APQ8-060820/5918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5919
apq8098					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5920
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5923
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may	H-QUA-APQ8-060820/5924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	-2020-bulletin	
msm8953					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5926
Improper Restriction of	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video	https://www.qualcomm.com/com	H-QUA-MSM8-060820/5927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	pany/product-security/bulletins/may-2020-bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5930
msm8998					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5933
nicobar					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-NICO-060820/5934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-NICO-060820/5935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-NICO-060820/5936
apq8053					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5937
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3616		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5940
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may	H-QUA-APQ8-060820/5941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	-2020-bulletin	
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5943
mdm9207c					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5945
Improper Restriction	02-06-2020	4.6	Possibility of out of bound access while processing the	https://www.qualcom	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	m.com/company/product-security/bulletins/may-2020-bulletin	060820/5946
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MDM9-060820/5948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
msm8905					
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/5949
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may	H-QUA-MSM8-060820/5950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	-2020-bulletin	
qcn7605					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCN7-060820/5951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCN7-060820/5952
sdm845					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no	https://www.qualcomm.com/company/product-	H-QUA-SDM8-060820/5953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	security/bulletins/may-2020-bulletin	
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM8-060820/5954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM8-060820/5955
Improper Restriction of Operations	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon	https://www.qualcomm.com/company/produ	H-QUA-SDM8-060820/5956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	ct-security/bulletins/may-2020-bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM8-060820/5957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM8-060820/5958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM8-060820/5959
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM8-060820/5960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**		
apq8017					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5961
apq8096au					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-APQ8-060820/5962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	bulletin	
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5964
Improper Restriction of Operations within the Bounds of a Memory	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may	H-QUA-APQ8-060820/5965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	-2020-bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-APQ8-060820/5967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sda845					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDA8-060820/5968
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-SDA8-060820/5969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	bulletin	
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDA8-060820/5970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3645		
sdm636					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5971
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check	https://www.qualcomm.com/company/product-security/bulletins/may	H-QUA-SDM6-060820/5972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5974
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in	https://www.qualcomm.com/company/product-	H-QUA-SDM6-060820/5975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	security/bulletins/may-2020-bulletin	
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
sdm670					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3610**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5978
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SDM6-060820/5979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	lletins/may-2020-bulletin	
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/5981
sdm710					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM7-060820/5982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM7-060820/5983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM7-060820/5984
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in	https://www.qualcomm.com/company/product-	H-QUA-SDM7-060820/5985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	security/bulletins/may-2020-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM7-060820/5986
qca8081					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-06-2020	7.2	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081, SC8180X, SXR2130 **CVE ID : CVE-2020-3618**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCA8-060820/5987
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCA8-060820/5988
qcs404					
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of	https://www.qualcomm.com/com	H-QUA-QCS4-060820/5989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	pany/product-security/bulletins/may-2020-bulletin	
sxr1130					
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SXR1-060820/5990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SXR1-060820/5991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SXR1-060820/5992
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SXR1-060820/5993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**		
sm6150					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM61-060820/5994
Buffer Copy without Checking	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking	https://www.qualcomm.com/com	H-QUA-SM61-060820/5995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	pany/product-security/bulletins/may-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM61-060820/5996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM61-060820/5997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM61-060820/5998
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM61-060820/5999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
sm8150					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM81-060820/6000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM81-060820/6001
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM81-060820/6002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM81-060820/6003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM81-060820/6004
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SM81-060820/6005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	lletins/may-2020-bulletin	
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM81-060820/6006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
qm215					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QM21-060820/6007
Buffer Copy without	02-06-2020	7.2	Buffer overflow in display function due to memory	https://www.qualcom	H-QUA-QM21-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	m.com/company/product-security/bulletins/may-2020-bulletin	060820/6008
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QM21-060820/6009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QM21-060820/6010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3633		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QM21-060820/6011
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QM21-060820/6012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**		
sm7150					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM71-060820/6013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM71-060820/6014
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM71-060820/6015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM71-060820/6016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM71-060820/6017
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM71-060820/6018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
sdm429					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/6019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/6020
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/6021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/6022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/6023
Time-of-check Time-	02-06-2020	6.9	A race condition can occur when using the fastrpc	https://www.qualcom	H-QUA-SDM4-060820/6024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of-use (TOCTOU) Race Condition			memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	m.com/company/product-security/bulletins/may-2020-bulletin	
sdm632					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/6025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/6026
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-SDM6-060820/6027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/6028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM6-060820/6029
Time-of-	02-06-2020	6.9	A race condition can occur	https://ww	H-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
check Time-of-use (TOCTOU) Race Condition			when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	w.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	060820/6030
msm8917					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/6031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/6032
Improper Restriction of Operations within the Bounds of a Memory	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may	H-QUA-MSM8-060820/6033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	-2020-bulletin	
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/6034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/6035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/6036
msm8996					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-MSM8-060820/6037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
sdm450					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/6038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150 **CVE ID : CVE-2020-3616**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/6039
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/6040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/6041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDM4-060820/6042
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SDM4-060820/6043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	lletins/may-2020-bulletin	
sm8250					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM82-060820/6044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Improper Input Validation	02-06-2020	7.2	kernel failure due to load failures while running v1 path directly via kernel in Snapdragon Mobile in SM8250, SXR2130 **CVE ID : CVE-2020-3623**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM82-060820/6045
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	When making query to DSP capabilities, Stack out of bounds occurs due to wrong buffer length configured for DSP attributes in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in SM8250, SXR2130 **CVE ID : CVE-2020-3625**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM82-060820/6046
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM82-060820/6047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM82-060820/6048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SM82-060820/6049
sxr2130					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-SXR2-060820/6050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	bulletin	
Use After Free	02-06-2020	7.2	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081, SC8180X, SXR2130 **CVE ID : CVE-2020-3618**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SXR2-060820/6051
Improper Input Validation	02-06-2020	7.2	kernel failure due to load failures while running v1 path directly via kernel in Snapdragon Mobile in SM8250, SXR2130 **CVE ID : CVE-2020-3623**	https://www.qualcomm.com/company/product-security/bulletins/may	H-QUA-SXR2-060820/6052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-06-2020	7.2	When making query to DSP capabilities, Stack out of bounds occurs due to wrong buffer length configured for DSP attributes in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in SM8250, SXR2130 **CVE ID : CVE-2020-3625**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SXR2-060820/6053
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SXR2-060820/6054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SXR2-060820/6055
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-SXR2-060820/6056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	bulletin	
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SXR2-060820/6057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
sa6155p					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SA61-060820/6058
Integer Overflow or	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper	https://www.qualcomm.com/com	H-QUA-SA61-060820/6059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	pany/product-security/bulletins/may-2020-bulletin	
sc8180x					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SC81-060820/6060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**		
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SC81-060820/6061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Use After Free	02-06-2020	7.2	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081, SC8180X, SXR2130 **CVE ID : CVE-2020-3618**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SC81-060820/6062
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SC81-060820/6063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SC81-060820/6064
sdm850					
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-SDM8-060820/6065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	bulletin	
qcm2150					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCM2-060820/6066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCM2-060820/6067
sdx55					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDX5-060820/6068
Reachable Assertion	02-06-2020	7.5	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDX5-060820/6069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3615**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SDX5-060820/6070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
rennell					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-RENN-060820/6071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-RENN-060820/6072
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-RENN-060820/6073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**	bulletin	
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-RENN-060820/6074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**		
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-RENN-060820/6075
sa415m					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-SA41-060820/6076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SA41-060820/6077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Time-of-check Time-of-use (TOCTOU) Race Condition	02-06-2020	6.9	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130 **CVE ID : CVE-2020-3680**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SA41-060820/6078
saipan					
Double Free	02-06-2020	4.6	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/may	H-QUA-SAIP-060820/6079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3610**	-2020-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SAIP-060820/6080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SAIP-060820/6081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-SAIP-060820/6082
ipq6018					
Use After Free	02-06-2020	7.2	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-	H-QUA-IPQ6-060820/6083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SXR2130 **CVE ID : CVE-2020-3618**	bulletin	
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-IPQ6-060820/6084
kamorta					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-06-2020	4.6	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-KAMO-060820/6085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3630**		
Improper Validation of Array Index	02-06-2020	10	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-KAMO-060820/6086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3633**		
Integer Overflow or Wraparound	02-06-2020	10	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3641**	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-KAMO-060820/6087
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in	https://www.qualcomm.com/company/product-	H-QUA-KAMO-060820/6088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**	security/bulletins/may-2020-bulletin	
qca6390					
Reachable Assertion	02-06-2020	7.8	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin	H-QUA-QCA6-060820/6089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2020-3645**		
ruckussecurity					
zonedirector_1200					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-RUC-ZONE-060820/6090
Samsung					
exynos_7570					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-06-2020	7.5	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (Exynos 7570 chipsets) software. The Trustonic Kinibi component allows arbitrary memory mapping. The Samsung ID is SVE-2019-16665 (June 2020). **CVE ID : CVE-2020-13831**	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-EXYN-060820/6091
sane-project					
sane_backends					
NULL Pointer Dereference	01-06-2020	2.1	A NULL pointer dereference in sanei_epson_net_read in SANE Backends before	https://alioth-lists.debian.	H-SAN-SANE-060820/6092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.30 allows a malicious device connected to the same local network as the victim to cause a denial of service, aka GHSL-2020-075. **CVE ID : CVE-2020-12867**	net/pipermail/sane-announce/2020/000041.html, https://gitlab.com/sane-project/backends/-/issues/279#issue-1-ghsl-2020-075-null-pointer-dereference-in-sanei_epson_net_read	
Siemens					
simatic_s7-150					
Unquoted Search Path or Element	10-06-2020	7.2	A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All	N/A	H-SIE-SIMA-060820/6093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. **CVE ID : CVE-2020-7580**		
logo\!_8_bm					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	10-06-2020	6.4	A vulnerability has been identified in LOGO!8 BM (incl. SIPLUS variants) (All versions). The vulnerability could lead to an attacker reading and modifying the device configuration and obtain project files from affected devices. The security vulnerability could be exploited by an unauthenticated attacker with network access to port 135/tcp. No user interaction is required to exploit this security vulnerability. The vulnerability impacts confidentiality, integrity, and availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known. **CVE ID : CVE-2020-7589**	N/A	H-SIE-LOGO-060820/6094
sokkia					
gnr5_vanguard					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-06-2020	7.5	SOKKIA GNR5 Vanguard WEB version 1.2 (build: 91f2b2c3a04d203d79862f87e2440cb7cefc3cd3) and hardware version 212 allows remote attackers to bypass admin authentication via a SQL injection attack that uses the User Name or Password field on the login page. **CVE ID : CVE-2020-14054**	N/A	H-SOK-GNR5-060820/6095
Sony					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wf-1000x					
Missing Authenticati on for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	H-SON-WF-1-060820/6096
wf-sp700n					
Missing Authenticati on for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	H-SON-WF-S-060820/6097
wh-1000xm2					
Missing Authenticati on for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-	N/A	H-SON-WH-1-060820/6098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**		
wh-1000xm3					
Missing Authenticati on for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	H-SON-WH-1-060820/6099
wh-ch700n					
Missing Authenticati on for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing	N/A	H-SON-WH-C-060820/6100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			volume of the product. **CVE ID : CVE-2020-5589**		
wh-h900n					
Missing Authenticati on for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	H-SON-WH-H-060820/6101
wh-xb700					
Missing Authenticati on for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	H-SON-WH-X-060820/6102
wh-xb900n					
Missing Authenticati on for	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-	N/A	H-SON-WH-X-060820/6103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Function			1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**		
wi-1000x					
Missing Authentication for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	H-SON-WI-1-060820/6104
wi-c600n					
Missing Authentication for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the	N/A	H-SON-WI-C-060820/6105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**		
wi-sp600n					
Missing Authenticati on for Critical Function	09-06-2020	8.3	SONY Wireless Headphones WF-1000X, WF-SP700N, WH-1000XM2, WH-1000XM3, WH-CH700N, WH-H900N, WH-XB700, WH-XB900N, WI-1000X, WI-C600N and WI-SP600N with firmware versions prior to 4.5.2 have vulnerability that someone within the Bluetooth range can make the Bluetooth pairing and operate such as changing volume of the product. **CVE ID : CVE-2020-5589**	N/A	H-SON-WI-S-060820/6106
Tp-link					
archer_c50					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-TP--ARCH-060820/6107
Trendnet					
tew-827dru					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	15-06-2020	6.5	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action kick_ban_wifi_mac_allow with a sufficiently long qcawifi.wifi0_vap0.maclist key. **CVE ID : CVE-2020-14074**	N/A	H-TRE-TEW--060820/6108
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	15-06-2020	9	TRENDnet TEW-827DRU devices through 2.06B04 contain multiple command injections in apply.cgi via the action pppoe_connect, ru_pppoe_connect, or dhcp_connect with the key wan_ifname (or wan0_dns), allowing an authenticated user to run arbitrary commands on the device. **CVE ID : CVE-2020-14075**	N/A	H-TRE-TEW--060820/6109
Out-of-bounds Write	15-06-2020	6.5	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action st_dev_connect, st_dev_disconnect, or st_dev_rconnect with a sufficiently long wan_type key.	N/A	H-TRE-TEW--060820/6110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14076		
Out-of-bounds Write	15-06-2020	6.5	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action set_sta_enrollee_pin_wifi1 (or set_sta_enrollee_pin_wifi0) with a sufficiently long wps_sta_enrollee_pin key. **CVE ID : CVE-2020-14077**	N/A	H-TRE-TEW--060820/6111
Out-of-bounds Write	15-06-2020	6.5	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action wifi_captive_portal_login with a sufficiently long REMOTE_ADDR key. **CVE ID : CVE-2020-14078**	N/A	H-TRE-TEW--060820/6112
Out-of-bounds Write	15-06-2020	6.5	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action auto_up_fw (or auto_up_lp) with a sufficiently long	N/A	H-TRE-TEW--060820/6113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update_file_name key. **CVE ID : CVE-2020-14079**		
Out-of-bounds Write	15-06-2020	7.5	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an unauthenticated user to execute arbitrary code by POSTing to apply_sec.cgi via the action ping_test with a sufficiently long ping_ipaddr key. **CVE ID : CVE-2020-14080**	N/A	H-TRE-TEW--060820/6114
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	15-06-2020	9	TRENDnet TEW-827DRU devices through 2.06B04 contain multiple command injections in apply.cgi via the action send_log_email with the key auth_acname (or auth_passwd), allowing an authenticated user to run arbitrary commands on the device. **CVE ID : CVE-2020-14081**	N/A	H-TRE-TEW--060820/6115
usavisionsys					
geovision_gv-as210					
Use of Hard-coded Credentials	12-06-2020	10	GeoVision Door Access Control device family is hardcoded with a root password, which adopting an identical password in all devices. **CVE ID : CVE-2020-3928**	N/A	H-USA-GEOV-060820/6116
Inadequate Encryption Strength	12-06-2020	4.3	GeoVision Door Access Control device family employs shared cryptographic private keys	N/A	H-USA-GEOV-060820/6117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext recover of encrypted messages. **CVE ID : CVE-2020-3929**		
geovision_gv-as410					
Use of Hard-coded Credentials	12-06-2020	10	GeoVision Door Access Control device family is hardcoded with a root password, which adopting an identical password in all devices. **CVE ID : CVE-2020-3928**	N/A	H-USA-GEOV-060820/6118
Inadequate Encryption Strength	12-06-2020	4.3	GeoVision Door Access Control device family employs shared cryptographic private keys for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext recover of encrypted messages. **CVE ID : CVE-2020-3929**	N/A	H-USA-GEOV-060820/6119
geovision_gv-as810					
Use of Hard-coded Credentials	12-06-2020	10	GeoVision Door Access Control device family is hardcoded with a root password, which adopting an identical password in all devices. **CVE ID : CVE-2020-3928**	N/A	H-USA-GEOV-060820/6120
Inadequate Encryption Strength	12-06-2020	4.3	GeoVision Door Access Control device family employs shared cryptographic private keys	N/A	H-USA-GEOV-060820/6121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext recover of encrypted messages. **CVE ID : CVE-2020-3929**		
geovision_gv-as1010					
Use of Hard-coded Credentials	12-06-2020	10	GeoVision Door Access Control device family is hardcoded with a root password, which adopting an identical password in all devices. **CVE ID : CVE-2020-3928**	N/A	H-USA-GEOV-060820/6122
Inadequate Encryption Strength	12-06-2020	4.3	GeoVision Door Access Control device family employs shared cryptographic private keys for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext recover of encrypted messages. **CVE ID : CVE-2020-3929**	N/A	H-USA-GEOV-060820/6123
geovision_gv-gf192x					
Use of Hard-coded Credentials	12-06-2020	10	GeoVision Door Access Control device family is hardcoded with a root password, which adopting an identical password in all devices. **CVE ID : CVE-2020-3928**	N/A	H-USA-GEOV-060820/6124
Inadequate Encryption Strength	12-06-2020	4.3	GeoVision Door Access Control device family employs shared cryptographic private keys	N/A	H-USA-GEOV-060820/6125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext recover of encrypted messages. **CVE ID : CVE-2020-3929**		
Information Exposure	12-06-2020	2.1	GeoVision Door Access Control device family improperly stores and controls access to system logs, any users can read these logs. **CVE ID : CVE-2020-3930**	N/A	H-USA-GEOV-060820/6126
Wago					
pfc200					
Improper Privilege Management	11-06-2020	9	An exploitable code execution vulnerability exists in the Web-Based Management (WBM) functionality of WAGO PFC 200 03.03.10(15). A specially crafted series of HTTP requests can cause code execution resulting in remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6090**	N/A	H-WAG-PFC2-060820/6127
ZTE					
zxv10_w300					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL	N/A	H-ZTE-ZXV1-060820/6128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		
f680					
Improper Input Validation	01-06-2020	3.3	ZTE's PON terminal product is impacted by the access control vulnerability. Due to the system not performing correct access control on some program interfaces, an attacker could use this vulnerability to tamper with the program interface parameters to perform unauthenticated operations. This affects: <ZTE F680><V9.0.10P1N6> **CVE ID : CVE-2020-6868**	N/A	H-ZTE-F680-060820/6129
Zyxel					
amg1202-t10b					
Incorrect Default Permissions	08-06-2020	7.8	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**	N/A	H-ZYX-AMG1-060820/6130
vmg8324-b10a					
Incorrect Default	08-06-2020	7.8	The Open Connectivity Foundation UPnP	N/A	H-ZYX-VMG8-060820/6131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue. **CVE ID : CVE-2020-12695**		