Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
74cms					
74cms					
N/A	02-Dec-20	7.5	PHP remote file inclusion in the assign_resume_tpl method in Application/Common/Controller/BaseController.class.php in 74CMS before 6.0.48 allows remote code execution. **CVE ID : CVE-2020-29279**	N/A	A-74C-74CM-171220/1
Acdsee					
photo_studio_2021					
N/A	07-Dec-20	7.5	PlugIns\IDE_ACDStd.apl in ACDSee Photo Studio Studio Professional 2021 14.0 Build 1705 has a User Mode Write AV starting at IDE_ACDStd!JPEGTransW+0x00000000000031aa. **CVE ID : CVE-2020-29595**	N/A	A-ACD-PHOT-171220/2
Adobe					
experience_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	3.5	AEM's Cloud Service offering, as well as versions 6.5.6.0 (and below), 6.4.8.2 (and below) and 6.3.3.8 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an	https://helpx.adobe.com/security/products/experience-manager/apsb20-72.html	A-ADO-EXPE-171220/3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2020-24445**		
prelude					
Uncontrolled Search Path Element	11-Dec-20	3.7	Adobe Prelude version 9.0.1 (and earlier) is affected by an uncontrolled search path element that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2020-24440**	https://helpx.adobe.com/security/products/prelude/apsb20-70.html	A-ADO-PREL-171220/4
experience_manager_forms_add-on					
Server-Side Request Forgery (SSRF)	10-Dec-20	5	AEM Forms SP6 add-on for AEM 6.5.6.0 and Forms add-on package for AEM 6.4 Service Pack 8 Cumulative Fix Pack 2 (6.4.8.2) have a blind Server-Side Request Forgery (SSRF) vulnerability. This vulnerability could be exploited by an unauthenticated attacker to gather information about internal systems that reside on the same network. **CVE ID : CVE-2020-24444**	https://helpx.adobe.com/security/products/experience-manager/apsb20-72.html	A-ADO-EXPE-171220/5
experience_manager_cloud_service					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	3.5	AEM's Cloud Service offering, as well as versions 6.5.6.0 (and below), 6.4.8.2 (and below) and 6.3.3.8 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2020-24445**	https://helpx.adobe.com/security/products/experience-manager/apsb20-72.html	A-ADO-EXPE-171220/6
lightroom					
Uncontrolled Search Path Element	11-Dec-20	3.7	Adobe Lightroom Classic version 10.0 (and earlier) for Windows is affected by an uncontrolled search path vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2020-24447**	https://helpx.adobe.com/security/products/lightroom/apsb20-74.html	A-ADO-LIGH-171220/7
advancedsystemcare					
advanced_systemcare					
N/A	03-Dec-20	4.9	There is a local denial of service vulnerability in Advanced SystemCare 13 PRO 13.5.0.174. Attackers can use a constructed	N/A	A-ADV-ADVA-171220/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			program to cause a computer crash (BSOD) **CVE ID : CVE-2020-23738**		
Almico					
speedfan					
Improper Privilege Management	03-Dec-20	4.6	There is a local privilege escalation vulnerability in Alfredo Milani Comparetti SpeedFan 4.52. Attackers can use constructed programs to increase user privileges **CVE ID : CVE-2020-28175**	N/A	A-ALM-SPEE-171220/9
altran					
picotcp					
Out-of-bounds Read	11-Dec-20	5	An issue was discovered in picoTCP and picoTCP-NG through 1.7.0. The DNS domain name record decompression functionality in pico_dns_decompress_name() in pico_dns_common.c does not validate the compression pointer offset values with respect to the actual data present in a DNS response packet, causing out-of-bounds reads that lead to Denial-of-Service. **CVE ID : CVE-2020-24339**	N/A	A-ALT-PICO-171220/10
Out-of-bounds Read	11-Dec-20	5	An issue was discovered in picoTCP and picoTCP-NG through 1.7.0. The code that processes DNS responses in pico_mdns_handle_data_as_answers_generic() in	N/A	A-ALT-PICO-171220/11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pico_mdns.c does not check whether the number of answers/responses specified in a DNS packet header corresponds to the response data available in the packet, leading to an out-of-bounds read, invalid pointer dereference, and Denial-of-Service. **CVE ID : CVE-2020-24340**		
Out-of-bounds Read	11-Dec-20	6.4	An issue was discovered in picoTCP and picoTCP-NG through 1.7.0. The TCP input data processing function in pico_tcp.c does not validate the length of incoming TCP packets, which leads to an out-of-bounds read when assembling received packets into a data segment, eventually causing Denial-of-Service or an information leak. **CVE ID : CVE-2020-24341**	N/A	A-ALT-PICO-171220/12
Out-of-bounds Read	11-Dec-20	6.4	An issue was discovered in picoTCP 1.7.0. The code for processing the IPv6 headers does not validate whether the IPv6 payload length field is equal to the actual size of the payload, which leads to an Out-of-Bounds read during the ICMPv6 checksum calculation, resulting in either Denial-of-Service or Information Disclosure. This affects pico_ipv6_extension_headers	N/A	A-ALT-PICO-171220/13

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and pico_checksum_adder (in pico_ipv6.c and pico_frame.c). **CVE ID : CVE-2020-17441**		
Integer Overflow or Wraparound	11-Dec-20	5	An issue was discovered in picoTCP 1.7.0. The code for parsing the hop-by-hop IPv6 extension headers does not validate the bounds of the extension header length value, which may result in Integer Wraparound. Therefore, a crafted extension header length value may cause Denial-of-Service because it affects the loop in which the extension headers are parsed in pico_ipv6_process_hopbyhop () in pico_ipv6.c. **CVE ID : CVE-2020-17442**	N/A	A-ALT-PICO-171220/14
Integer Overflow or Wraparound	11-Dec-20	5	An issue was discovered in picoTCP 1.7.0. The code for creating an ICMPv6 echo replies doesn't check whether the ICMPv6 echo request packet's size is shorter than 8 bytes. If the size of the incoming ICMPv6 request packet is shorter than this, the operation that calculates the size of the ICMPv6 echo replies has an integer wrap around, leading to memory corruption and, eventually, Denial-of-Service in pico_icmp6_send_echoreply_not_frag in pico_icmp6.c.	N/A	A-ALT-PICO-171220/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-17443		
Integer Overflow or Wraparound	11-Dec-20	5	An issue was discovered in picoTCP 1.7.0. The routine for processing the next header field (and deducing whether the IPv6 extension headers are valid) doesn't check whether the header extension length field would overflow. Therefore, if it wraps around to zero, iterating through the extension headers will not increment the current data pointer. This leads to an infinite loop and Denial-of-Service in pico_ipv6_check_headers_sequence() in pico_ipv6.c. **CVE ID : CVE-2020-17444**	N/A	A-ALT-PICO-171220/16
Out-of-bounds Read	11-Dec-20	5	An issue was discovered in picoTCP 1.7.0. The code for processing the IPv6 destination options does not check for a valid length of the destination options header. This results in an Out-of-Bounds Read, and, depending on the memory protection mechanism, this may result in Denial-of-Service in pico_ipv6_process_destopt() in pico_ipv6.c. **CVE ID : CVE-2020-17445**	N/A	A-ALT-PICO-171220/17
Loop with Unreachable Exit Condition	11-Dec-20	5	An issue was discovered in picoTCP and picoTCP-NG through 1.7.0. When an unsupported TCP option	N/A	A-ALT-PICO-171220/18

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			with zero length is provided in an incoming TCP packet, it is possible to cause a Denial-of-Service by achieving an infinite loop in the code that parses TCP options, aka tcp_parse_options() in pico_tcp.c. **CVE ID : CVE-2020-24337**		
Out-of-bounds Write	11-Dec-20	7.5	An issue was discovered in picoTCP through 1.7.0. The DNS domain name record decompression functionality in pico_dns_decompress_name() in pico_dns_common.c does not validate the compression pointer offset values with respect to the actual data present in a DNS response packet, causing out-of-bounds writes that lead to Denial-of-Service and Remote Code Execution. **CVE ID : CVE-2020-24338**	N/A	A-ALT-PICO-171220/19
picotcp-ng					
Out-of-bounds Read	11-Dec-20	5	An issue was discovered in picoTCP and picoTCP-NG through 1.7.0. The DNS domain name record decompression functionality in pico_dns_decompress_name() in pico_dns_common.c does not validate the compression pointer offset values with respect to the actual data present in a DNS response packet, causing out-of-	N/A	A-ALT-PICO-171220/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bounds reads that lead to Denial-of-Service. **CVE ID : CVE-2020-24339**		
Out-of-bounds Read	11-Dec-20	5	An issue was discovered in picoTCP and picoTCP-NG through 1.7.0. The code that processes DNS responses in pico_mdns_handle_data_as_answers_generic() in pico_mdns.c does not check whether the number of answers/responses specified in a DNS packet header corresponds to the response data available in the packet, leading to an out-of-bounds read, invalid pointer dereference, and Denial-of-Service. **CVE ID : CVE-2020-24340**	N/A	A-ALT-PICO-171220/21
Out-of-bounds Read	11-Dec-20	6.4	An issue was discovered in picoTCP and picoTCP-NG through 1.7.0. The TCP input data processing function in pico_tcp.c does not validate the length of incoming TCP packets, which leads to an out-of-bounds read when assembling received packets into a data segment, eventually causing Denial-of-Service or an information leak. **CVE ID : CVE-2020-24341**	N/A	A-ALT-PICO-171220/22
Loop with Unreachable Exit Condition	11-Dec-20	5	An issue was discovered in picoTCP and picoTCP-NG through 1.7.0. When an unsupported TCP option	N/A	A-ALT-PICO-171220/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			with zero length is provided in an incoming TCP packet, it is possible to cause a Denial-of-Service by achieving an infinite loop in the code that parses TCP options, aka tcp_parse_options() in pico_tcp.c. **CVE ID : CVE-2020-24337**		
amoisoft					
anyview					
N/A	03-Dec-20	4.9	In AnyView (network police) network monitoring software 4.6.0.1, there is a local denial of service vulnerability in AnyView, attackers can use a constructed program to cause a computer crash (BSOD). **CVE ID : CVE-2020-23741**	N/A	A-AMO-ANYV-171220/24
Antiy					
antiy_zhijia_terminal_defense_system					
N/A	03-Dec-20	4.9	There is a local denial of service vulnerability in the Antiy Zhijia Terminal Defense System 5.0.2.10121559 and an attacker can cause a computer crash (BSOD). **CVE ID : CVE-2020-23727**	N/A	A-ANT-ANTI-171220/25
anydesk					
anydesk					
Improper Privilege Management	09-Dec-20	7.2	AnyDesk for macOS versions 6.0.2 and older have a vulnerability in the XPC	N/A	A-ANY-ANYD-171220/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface that does not properly validate client requests and allows local privilege escalation. **CVE ID : CVE-2020-27614**		
Apache					
tomcat					
Information Exposure	03-Dec-20	5	While investigating bug 64830 it was discovered that Apache Tomcat 10.0.0-M1 to 10.0.0-M9, 9.0.0-M1 to 9.0.39 and 8.5.0 to 8.5.59 could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream. While this would most likely lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak between requests. **CVE ID : CVE-2020-17527**	https://security.netapp.com/advisory/ntap-20201210-0003/	A-APA-TOMC-171220/27
airflow					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	4.3	The "origin" parameter passed to some of the endpoints like '/trigger' was vulnerable to XSS exploit. This issue affects Apache Airflow versions prior to 1.10.13. This is same as CVE-2020-13944 but the implemented fix in Airflow 1.10.13 did not fix the issue completely.	N/A	A-APA-AIRF-171220/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-17515		
storm_docker					
N/A	08-Dec-20	10	The official storm Docker images before 1.2.1 contain a blank password for a root user. Systems using the Storm Docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-29580**	N/A	A-APA-STOR-171220/29
groovy					
N/A	07-Dec-20	2.1	Apache Groovy provides extension methods to aid with creating temporary directories. Prior to this fix, Groovy's implementation of those extension methods was using a now superseded Java JDK method call that is potentially not secure on some operating systems in some contexts. Users not using the extension methods mentioned in the advisory are not affected, but may wish to read the advisory for further details. Versions Affected: 2.0 to 2.4.20, 2.5.0 to 2.5.13, 3.0.0 to 3.0.6, and 4.0.0-alpha-1. Fixed in versions 2.4.21, 2.5.14, 3.0.7, 4.0.0-alpha-2. **CVE ID : CVE-2020-17521**	https://groovy-lang.org/security.html#CVE-2020-17521	A-APA-GROO-171220/30
struts					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	11-Dec-20	7.5	Forced OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution. Affected software : Apache Struts 2.0.0 - Struts 2.5.25. **CVE ID : CVE-2020-17530**	https://cwiki.apache.org/confluence/display/WW/S2-061	A-APA-STRU-171220/31
cordova					
N/A	01-Dec-20	2.1	We have resolved a security issue in the camera plugin that could have affected certain Cordova (Android) applications. An attacker who could install (or lead the victim to install) a specially crafted (or malicious) Android application would be able to access pictures taken with the app externally. **CVE ID : CVE-2020-11990**	N/A	A-APA-CORD-171220/32
apisix					
N/A	07-Dec-20	4	In Apache APISIX, the user enabled the Admin API and deleted the Admin API access IP restriction rules. Eventually, the default token is allowed to access APISIX management data. This affects versions 1.2, 1.3, 1.4, 1.5. **CVE ID : CVE-2020-13945**	https://lists.apache.org/thread.html/r792feb29964067a4108f53e8579a1e9bd1c8b5b9bc95618c814faf2f%40%3Cdev.apisix.apache.org%3E	A-APA-APIS-171220/33
httpclient					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Dec-20	5	Apache HttpClient versions prior to version 4.5.13 and 5.0.3 can misinterpret malformed authority component in request URIs passed to the library as java.net.URI object and pick the wrong target host for request execution. **CVE ID : CVE-2020-13956**	N/A	A-APA-HTTP-171220/34
tapestry					
Deserialization of Untrusted Data	08-Dec-20	7.5	A Java Serialization vulnerability was found in Apache Tapestry 4. Apache Tapestry 4 will attempt to deserialize the "sp" parameter even before invoking the page's validate method, leading to deserialization without authentication. Apache Tapestry 4 reached end of life in 2008 and no update to address this issue will be released. Apache Tapestry 5 versions are not vulnerable to this issue. Users of Apache Tapestry 4 should upgrade to the latest Apache Tapestry 5 version. **CVE ID : CVE-2020-17531**	N/A	A-APA-TAPE-171220/35
Apereo					
opencast					
Origin Validation Error	08-Dec-20	2.1	Opencast before versions 8.9 and 7.9 disables HTTPS hostname verification of its HTTP client used for a large portion of Opencast's HTTP	https://github.com/opencast/opencast/security/advisorie	A-APE-OPEN-171220/36

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests. Hostname verification is an important part when using HTTPS to ensure that the presented certificate is valid for the host. Disabling it can allow for man-in-the-middle attacks. This problem is fixed in Opencast 7.9 and Opencast 8.8 Please be aware that fixing the problem means that Opencast will not simply accept any self-signed certificates any longer without properly importing them. If you need those, please make sure to import them into the Java key store. Better yet, get a valid certificate. **CVE ID : CVE-2020-26234**	s/GHSA-44cw-p2hm-gpf6	
appimage					
libappimage					
N/A	02-Dec-20	4.3	AppImage libappimage before 1.0.3 allows attackers to trigger an overwrite of a system-installed .desktop file by providing a .desktop file that contains Name= with path components. **CVE ID : CVE-2020-25265**	N/A	A-APP-LIBA-171220/37
appimaged					
Download of Code Without Integrity Check	02-Dec-20	4.3	AppImage appimaged before 1.0.3 does not properly check whether a downloaded file is a valid appimage. For example, it	N/A	A-APP-APPI-171220/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			will accept a crafted mp3 file that contains an appimage, and install it. **CVE ID : CVE-2020-25266**		
Apple					
icloud					
N/A	08-Dec-20	2.1	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A local user may be able to read arbitrary files. **CVE ID : CVE-2020-10002**	https://support.apple.com/kb/HT212011	A-APP-ICLO-171220/39
Integer Overflow or Wraparound	08-Dec-20	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-27911**	https://support.apple.com/kb/HT212011	A-APP-ICLO-171220/40
Out-of-bounds Write	08-Dec-20	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows.	https://support.apple.com/kb/HT212011	A-APP-ICLO-171220/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-27912**		
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-27917**	N/A	A-APP-ICLO-171220/42
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, Safari 14.0.1, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-27918**	N/A	A-APP-ICLO-171220/43
Access of Resource Using Incompatible Type ('Type Confusion')	08-Dec-20	9.3	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update	N/A	A-APP-ICLO-171220/44

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-27932**		
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, Safari 14.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9947**	N/A	A-APP-ICLO-171220/45
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted file may lead to arbitrary code execution.	N/A	A-APP-ICLO-171220/46

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9981		
N/A	08-Dec-20	5	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iCloud for Windows 7.21, tvOS 14.0. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9991**	N/A	A-APP-ICLO-171220/47
itunes					
N/A	08-Dec-20	2.1	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A local user may be able to read arbitrary files. **CVE ID : CVE-2020-10002**	https://support.apple.com/kb/HT212011	A-APP-ITUN-171220/48
Information Exposure	08-Dec-20	4.3	An information disclosure issue existed in the transition of program state. This issue was addressed with improved state handling. This issue is fixed in iTunes 12.11 for Windows. A malicious application may be able to access local users Apple IDs. **CVE ID : CVE-2020-27895**	N/A	A-APP-ITUN-171220/49
Integer Overflow or Wraparound	08-Dec-20	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Big Sur	https://support.apple.com/kb/HT2	A-APP-ITUN-171220/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-27911**	12011	
Out-of-bounds Write	08-Dec-20	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-27912**	https://support.apple.com/kb/HT212011	A-APP-ITUN-171220/51
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-27917**	N/A	A-APP-ITUN-171220/52
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS	N/A	A-APP-ITUN-171220/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			14.2 and iPadOS 14.2, iCloud for Windows 11.5, Safari 14.0.1, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-27918**		
Access of Resource Using Incompatible Type ('Type Confusion')	08-Dec-20	9.3	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-27932**	N/A	A-APP-ITUN-171220/54
Information Exposure	08-Dec-20	4.3	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0. A remote attacker may be able to leak memory.	N/A	A-APP-ITUN-171220/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9849		
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2020-9981**	N/A	A-APP-ITUN-171220/56
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Dec-20	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iTunes for Windows 12.10.9. Processing a maliciously crafted text file may lead to arbitrary code execution. **CVE ID : CVE-2020-9999**	N/A	A-APP-ITUN-171220/57
safari					
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, Safari 14.0.1, tvOS 14.2, iTunes 12.11 for Windows.	N/A	A-APP-SAFA-171220/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-27918**		
Improper Restriction of Rendered UI Layers or Frames	08-Dec-20	4.3	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, Safari 13.1.2. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2020-9942**	N/A	A-APP-SAFA-171220/59
Improper Restriction of Rendered UI Layers or Frames	08-Dec-20	4.3	A spoofing issue existed in the handling of URLs. This issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, Safari 14.0.1. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2020-9945**	N/A	A-APP-SAFA-171220/60
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, tvOS 14.0, Safari 14.0, iOS 14.0 and iPadOS 14.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9950**	N/A	A-APP-SAFA-171220/61
Improper Restriction	08-Dec-20	4.3	An inconsistent user interface issue was	N/A	A-APP-SAFA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Rendered UI Layers or Frames			addressed with improved state management. This issue is fixed in Safari 14.0. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2020-9987**		171220/62
Improper Restriction of Rendered UI Layers or Frames	08-Dec-20	4.3	The issue was addressed with improved UI handling. This issue is fixed in watchOS 7.0, Safari 14.0, iOS 14.0 and iPadOS 14.0. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2020-9993**	N/A	A-APP-SAFA-171220/63
arachnys					
cabot					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Dec-20	3.5	Cross Site Scripting (XSS) vulnerability in Arachnys Cabot 0.11.12 can be exploited via the Address column. **CVE ID : CVE-2020-25449**	N/A	A-ARA-CABO-171220/64
Artifex					
mupdf					
Use After Free	09-Dec-20	6.8	A Use After Free vulnerability exists in Artifex Software, Inc. MuPDF library 1.17.0-rc1 and earlier when a valid page was followed by a page with invalid pixmap dimensions, causing bander - a static - to point to previously freed memory	N/A	A-ART-MUPD-171220/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			instead of a newband_writer. **CVE ID : CVE-2020-16600**		
aswf					
openexr					
Out-of-bounds Write	09-Dec-20	4.3	A heap-based buffer overflow vulnerability exists in Academy Software Foundation OpenEXR 2.3.0 in chunkOffsetReconstruction in ImfMultiPartInputFile.cpp that can cause a denial of service via a crafted EXR file. **CVE ID : CVE-2020-16587**	N/A	A-ASW-OPEN-171220/66
NULL Pointer Dereference	09-Dec-20	4.3	A Null Pointer Deference issue exists in Academy Software Foundation OpenEXR 2.3.0 in generatePreview in makePreview.cpp that can cause a denial of service via a crafted EXR file. **CVE ID : CVE-2020-16588**	N/A	A-ASW-OPEN-171220/67
Out-of-bounds Write	09-Dec-20	4.3	A head-based buffer overflow exists in Academy Software Foundation OpenEXR 2.3.0 in writeTileData in ImfTiledOutputFile.cpp that can cause a denial of service via a crafted EXR file. **CVE ID : CVE-2020-16589**	N/A	A-ASW-OPEN-171220/68
Awstats					
awstats					
Improper Limitation of	07-Dec-20	7.5	In AWStats through 7.7, cgi-bin/awstats.pl?config=	N/A	A-AWS-AWST-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			accepts an absolute pathname, even though it was intended to only read a file in the /etc/awstats/awstats.conf format. NOTE: this issue exists because of an incomplete fix for CVE-2017-1000501. **CVE ID : CVE-2020-29600**		171220/69
bitrix24					
bitrix_framework					
Improper Restriction of Excessive Authentication Attempts	02-Dec-20	4	An issue was discovered in Bitrix24 Bitrix Framework (1c site management) 20.0. An "User enumeration and Improper Restriction of Excessive Authentication Attempts" vulnerability exists in the admin login form, allowing a remote user to enumerate users in the administrator group. This also allows brute-force attacks on the passwords of users not in the administrator group. **CVE ID : CVE-2020-28206**	N/A	A-BIT-BITR-171220/70
bloodx_project					
bloodx					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	02-Dec-20	7.5	SQL injection vulnerability in BloodX 1.0 allows attackers to bypass authentication. **CVE ID : CVE-2020-29282**	N/A	A-BLO-BLOO-171220/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')					
bookstackapp					
bookstack					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-Dec-20	5.5	BookStack is a platform for storing and organising information and documentation. In BookStack before version 0.30.5, a user with permissions to edit a page could set certain image URL's to manipulate functionality in the exporting system, which would allow them to make server side requests and/or have access to a wider scope of files within the BookStack file storage locations. The issue was addressed in BookStack v0.30.5. As a workaround, page edit permissions could be limited to only those that are trusted until you can upgrade. **CVE ID : CVE-2020-26260**	https://github.com/BookStackApp/BookStack/security/advisories/GHSA-8wfc-w2r5-x7cr	A-BOO-BOOK-171220/72
boom-core					
risvc-boom					
Missing Authorization	04-Dec-20	4.3	An issue was discovered in SonicBOOM riscv-boom 3.0.0. For LR, it does not avoid acquiring a reservation in the case where a load translates successfully but still generates an exception. **CVE ID : CVE-2020-29561**	N/A	A-BOO-RISV-171220/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Broadcom					
symantec_messaging_gateway					
Improper Privilege Management	10-Dec-20	9	A privilege escalation flaw allows a malicious, authenticated, privileged CLI user to escalate their privileges on the system and gain full control over the SMG appliance. This affects SMG prior to 10.7.4. **CVE ID : CVE-2020-12594**	https://support.broadcom.com/security-advisory/content/security-advisories/Privilege-Escalation-and-Information-Disclosure-Vulnerabilities-in-SMG/SYMSA16609	A-BRO-SYMA-171220/74
N/A	10-Dec-20	4	An information disclosure flaw allows a malicious, authenticated, privileged web UI user to obtain a password for a remote SCP backup server that they might not otherwise be authorized to access. This affects SMG prior to 10.7.4. **CVE ID : CVE-2020-12595**	https://support.broadcom.com/security-advisory/content/security-advisories/Privilege-Escalation-and-Information-Disclosure-Vulnerabilities-in-SMG/SYMSA16609	A-BRO-SYMA-171220/75
c2fo					
fast-csv					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	08-Dec-20	3.5	Fast-csv is an npm package for parsing and formatting CSVs or any other delimited value file in node. In fast-cvs before version 4.3.6 there is a possible ReDoS vulnerability (Regular Expression Denial of Service) when using ignoreEmpty option when parsing. This has been patched in `v4.3.6` You will only be affected by this if you use the `ignoreEmpty` parsing option. If you do use this option it is recommended that you upgrade to the latest version `v4.3.6` This vulnerability was found using a CodeQL query which identified `EMPTY_ROW_REGEXP` regular expression as vulnerable. **CVE ID : CVE-2020-26256**	https://github.com/C2FO/fast-csv/security/advisories/GHSA-8cv5-p934-3hwp	A-C2F-FAST-171220/76
Canonical					
snapcraft					
Uncontrolled Search Path Element	04-Dec-20	4.4	In some conditions, a snap package built by snapcraft includes the current directory in LD_LIBRARY_PATH, allowing a malicious snap to gain code execution within the context of another snap if both plug the home interface or similar. This issue affects snapcraft versions prior to 4.4.4, prior to	N/A	A-CAN-SNAP-171220/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.43.1+16.04.1, and prior to 2.43.1+18.04.1. **CVE ID : CVE-2020-27348**		
car_rental_management_system_project					
car_rental_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-20	7.5	An SQL injection vulnerability was discovered in Car Rental Management System v1.0 can be exploited via the id parameter in view_car.php or the car_id parameter in booking.php. **CVE ID : CVE-2020-29287**	N/A	A-CAR-CAR_-171220/78
Ceph					
ceph-ansible					
Cleartext Storage of Sensitive Information	08-Dec-20	2.1	Ceph-ansible 4.0.34.1 creates /etc/ceph/iscsi-gateway.conf with insecure default permissions, allowing any user to read the sensitive information within. **CVE ID : CVE-2020-25677**	https://bugzilla.redhat.com/show_bug.cgi?id=1892108, https://github.com/ceph/ceph-ansible/pull/5964	A-CEP-CEPH-171220/79
Checkpoint					
endpoint_security					
Uncontrolled Search Path Element	03-Dec-20	4.4	Check Point Endpoint Security Client for Windows before version E84.20 allows write access to the directory from which the installation repair takes place. Since the MS Installer allows regular users to run the repair, an attacker can initiate the	N/A	A-CHE-ENDP-171220/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installation repair and place a specially crafted DLL in the repair folder which will run with the Endpoint client's privileges. **CVE ID : CVE-2020-6021**		
cimg					
cimg					
Out-of-bounds Write	03-Dec-20	5.8	A flaw was found in CImg in versions prior to 2.9.3. Integer overflows leading to heap buffer overflows in load_pnm() can be triggered by a specially crafted input file processed by CImg, which can lead to an impact to application availability or data integrity. **CVE ID : CVE-2020-25693**	N/A	A-CIM-CIMG-171220/81
Cisco					
jabber					
Improper Privilege Management	11-Dec-20	9	Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-27132**	N/A	A-CIS-JABB-171220/82
Improper	11-Dec-20	9	Multiple vulnerabilities in	N/A	A-CIS-JABB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-27133**		171220/83
Improper Privilege Management	11-Dec-20	9	Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-27134**	N/A	A-CIS-JABB-171220/84
Improper Privilege Management	11-Dec-20	9	Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more	N/A	A-CIS-JABB-171220/85

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-27127**		
jabber_for_mobile_platforms					
Improper Privilege Management	11-Dec-20	9	Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-27132**	N/A	A-CIS-JABB-171220/86
Improper Privilege Management	11-Dec-20	9	Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-27133**	N/A	A-CIS-JABB-171220/87
Improper Privilege	11-Dec-20	9	Multiple vulnerabilities in Cisco Jabber for Windows,	N/A	A-CIS-JABB-171220/88

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-27134**		
Improper Privilege Management	11-Dec-20	9	Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-27127**	N/A	A-CIS-JABB-171220/89
classroombookings					
classroombookings					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	14-Dec-20	6.5	SQL Injection in Classbooking before 2.4.1 via the username field of a CSV file when adding a new user. **CVE ID : CVE-2020-35382**	N/A	A-CLA-CLAS-171220/90

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')					
cloudfoundry					
cf-deployment					
Uncontrolled Resource Consumption	02-Dec-20	7.8	CAPI (Cloud Controller) versions prior to 1.101.0 are vulnerable to a denial-of-service attack in which an unauthenticated malicious attacker can send specially-crafted YAML files to certain endpoints, causing the YAML parser to consume excessive CPU and RAM. **CVE ID : CVE-2020-5423**	https://www.cloudfoundry.org/blog/cve-2020-5423	A-CLO-CF-D-171220/91
capi-release					
Uncontrolled Resource Consumption	02-Dec-20	7.8	CAPI (Cloud Controller) versions prior to 1.101.0 are vulnerable to a denial-of-service attack in which an unauthenticated malicious attacker can send specially-crafted YAML files to certain endpoints, causing the YAML parser to consume excessive CPU and RAM. **CVE ID : CVE-2020-5423**	https://www.cloudfoundry.org/blog/cve-2020-5423	A-CLO-CAPI-171220/92
cogboard					
red-dashboard					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	3.5	Red Discord Bot Dashboard is an easy-to-use interactive web dashboard to control your Redbot. In Red Discord Bot before version 0.1.7a an RCE exploit has been discovered. This exploit allows Discord users with specially crafted Server	https://github.com/Cog-Creators/Red-Dashboard/security/advisories/GHSA-hm45-	A-COG-RED--171220/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			names and Usernames/Nicknames to inject code into the webserver front-end code. By abusing this exploit, it's possible to perform destructive actions and/or access sensitive information. This high severity exploit has been fixed on version 0.1.7a. There are no workarounds, bot owners must upgrade their relevant packages (Dashboard module and Dashboard webserver) in order to patch this issue. **CVE ID : CVE-2020-26249**	mgqm-gjm4	
corenlp-js-interface_project					
corenlp-js-interface					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	7.5	All versions of package corenlp-js-interface are vulnerable to Command Injection via the main function. **CVE ID : CVE-2020-28440**	https://snyk.io/vuln/SNYK-JS-CORENLPJSINTERFACE-1050435	A-COR-CORE-171220/94
corenlp-js-prefab_project					
corenlp-js-prefab					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	7.5	This affects all versions of package corenlp-js-prefab. The injection point is located in line 10 in 'index.js.' It depends on a vulnerable package 'corenlp-js-interface.' Vulnerability can be exploited with the	https://snyk.io/vuln/SNYK-JS-CORENLPJSPREFAB-1050434	A-COR-CORE-171220/95

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			following PoC: **CVE ID : CVE-2020-28439**		
crux					
crux					
Missing Authentication for Critical Function	02-Dec-20	10	The official Crux Linux Docker images 3.0 through 3.4 contain a blank password for a root user. System using the Crux Linux Docker container deployed by affected versions of the Docker image may allow an attacker to achieve root access with a blank password. **CVE ID : CVE-2020-29389**	N/A	A-CRU-CRUX-171220/96
ctolog					
thinkadmin					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-20	4.3	ThinkAdmin version v1 v6 has a stored XSS vulnerability which allows remote attackers to inject an arbitrary web script or HTML. **CVE ID : CVE-2020-29315**	N/A	A-CTO-THIN-171220/97
dadajiasu					
dada_accelerator					
N/A	03-Dec-20	4.9	There is a local denial of service vulnerability in DaDa accelerator 5.6.19.816,, attackers can use constructed programs to cause computer crashes (BSOD). **CVE ID : CVE-2020-23736**	N/A	A-DAD-DADA-171220/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Debian					
advanced_package_tool					
Integer Overflow or Wraparound	10-Dec-20	4.6	APT had several integer overflows and underflows while parsing .deb packages, aka GHSL-2020-168 GHSL-2020-169, in files apt-pkg/contrib/extracttar.cc, apt-pkg/deb/debfile.cc, and apt-pkg/contrib/arfile.cc. This issue affects: apt 1.2.32ubuntu0 versions prior to 1.2.32ubuntu0.2; 1.6.12ubuntu0 versions prior to 1.6.12ubuntu0.2; 2.0.2ubuntu0 versions prior to 2.0.2ubuntu0.2; 2.1.10ubuntu0 versions prior to 2.1.10ubuntu0.1; **CVE ID : CVE-2020-27350**	https://bugs.launchpad.net/bugs/1899193	A-DEB-ADVA-171220/99
Missing Release of Resource after Effective Lifetime	10-Dec-20	2.1	Various memory and file descriptor leaks were found in apt-python files python/arfile.cc, python/tag.cc, python/tarfile.cc, aka GHSL-2020-170. This issue affects: python-apt 1.1.0~beta1 versions prior to 1.1.0~beta1ubuntu0.16.04.10; 1.6.5ubuntu0 versions prior to 1.6.5ubuntu0.4; 2.0.0ubuntu0 versions prior to 2.0.0ubuntu0.20.04.2; 2.1.3ubuntu1 versions prior to 2.1.3ubuntu1.1; **CVE ID : CVE-2020-27351**	https://bugs.launchpad.net/bugs/1899193	A-DEB-ADVA-171220/100
deepref_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
deepref					
N/A	08-Dec-20	7.5	Prototype pollution vulnerability in 'deepref' versions 1.1.1 through 1.2.1 allows attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2020-28274**	https://www.whitesourcesoftware.com/vulnerability-database/CVE-2020-28274,https://github.com/isaymatato/deepref/commit/24935e6a1060cb09c641d3075982f0b44cfca4c2	A-DEE-DEEP-171220/101
desknets					
neo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Dec-20	4.3	Cross-site scripting vulnerability in desknet's NEO (desknet's NEO Small License V5.5 R1.5 and earlier, and desknet's NEO Enterprise License V5.5 R1.5 and earlier) allows remote attackers to inject arbitrary script via unspecified vectors. **CVE ID : CVE-2020-5638**	N/A	A-DES-NEO-171220/102
divebook_project					
divebook					
Missing Authorization	08-Dec-20	5	The DiveBook plugin 1.1.4 for WordPress is prone to improper access control in the Log Dive form because it fails to perform	N/A	A-DIV-DIVE-171220/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization checks. An attacker may leverage this issue to manipulate the integrity of dive logs. **CVE ID : CVE-2020-14205**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-20	4.3	The DiveBook plugin 1.1.4 for WordPress is prone to unauthenticated XSS within the filter function (via an arbitrary parameter). **CVE ID : CVE-2020-14206**	N/A	A-DIV-DIVE-171220/104
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Dec-20	5	The DiveBook plugin 1.1.4 for WordPress was prone to a SQL injection within divelog.php, allowing unauthenticated users to retrieve data from the database via the divelog.php filter_diver parameter. **CVE ID : CVE-2020-14207**	N/A	A-DIV-DIVE-171220/105
Docker					
regisry					
Improper Privilege Management	11-Dec-20	10	Versions of the Official registry Docker images through 2.7.0 contain a blank password for the root user. Systems deployed using affected versions of the registry container may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-29591**	N/A	A-DOC-REGI-171220/106
notary_docker_image					
N/A	08-Dec-20	10	The official notary docker	N/A	A-DOC-NOTA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			images before signer-0.6.1-1 contain a blank password for a root user. System using the notary docker container deployed by affected versions of the docker image may allow an remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-29601**		171220/107
drivergenius					
drivergenius					
Improper Privilege Management	03-Dec-20	4.6	In DriverGenius 9.61.5480.28 there is a local privilege escalation vulnerability in the driver wizard, attackers can use constructed programs to increase user privileges. **CVE ID : CVE-2020-23740**	N/A	A-DRI-DRIV-171220/108
druva					
insync					
Incorrect Default Permissions	07-Dec-20	7.2	inSync Client installer for macOS versions v6.8.0 and prior could allow an attacker to gain privileges of a root user from a lower privileged user due to improper integrity checks and directory permissions. **CVE ID : CVE-2020-5798**	N/A	A-DRU-INSY-171220/109
eat_spray_love_project					
eat_spray_love					
N/A	07-Dec-20	7.5	The Eat Spray Love mobile app for both iOS and	N/A	A-EAT-EAT_-171220/110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Android contains a backdoor account that, when modified, allowed privileged access to restricted functionality and to other users' data. **CVE ID : CVE-2020-5799**		
Improper Authenticati on	07-Dec-20	7.5	The Eat Spray Love mobile app for both iOS and Android contains logic that allows users to bypass authentication and retrieve or modify information that they would not normally have access to. **CVE ID : CVE-2020-5800**	N/A	A-EAT-EAT_-171220/111
Ec-cube					
ec-cube					
Improper Restriction of Rendered UI Layers or Frames	03-Dec-20	4.3	Improper restriction of rendered UI layers or frames in EC-CUBE versions from 3.0.0 to 3.0.18 leads to clickjacking attacks. If a user accesses a specially crafted page while logged into the administrative page, unintended operations may be conducted. **CVE ID : CVE-2020-5679**	N/A	A-EC--EC-C-171220/112
Improper Input Validation	03-Dec-20	5	Improper input validation vulnerability in EC-CUBE versions from 3.0.5 to 3.0.18 allows a remote attacker to cause a denial-of-service (DoS) condition via unspecified vector. **CVE ID : CVE-2020-5680**	N/A	A-EC--EC-C-171220/113
Eggheads					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
eggdrop_docker					
N/A	08-Dec-20	10	The official eggdrop Docker images before 1.8.4rc2 contain a blank password for a root user. Systems using the Eggdrop Docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-29576**	N/A	A-EGG-EGGD-171220/114
Elastic					
kibana					
URL Redirection to Untrusted Site ('Open Redirect')	02-Dec-20	5.8	The elasticsearch-operator does not validate the namespace where kibana logging resource is created and due to that it is possible to replace the original openshift-logging console link (kibana console) to different one, created based on the new CR for the new kibana resource. This could lead to an arbitrary URL redirection or the openshift-logging console link damage. This flaw affects elasticsearch-operator-container versions before 4.7. **CVE ID : CVE-2020-27816**	N/A	A-ELA-KIBA-171220/115
elixir-lang					
docker_image					
N/A	08-Dec-20	10	The official elixir Docker	N/A	A-ELI-DOCK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			images before 1.8.0-alpine (Alpine specific) contain a blank password for a root user. Systems using the elixir Linux Docker container deployed by affected versions of the Docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-29575**		171220/116
ethereum					
go_ethereum					
Uncontrolled Resource Consumption	11-Dec-20	4	Go Ethereum, or "Geth", is the official Golang implementation of the Ethereum protocol. In Geth before version 1.9.25 a denial-of-service vulnerability can make a LES server crash via malicious GetProofsV2 request from a connected LES client. This vulnerability only concerns users explicitly enabling les server; disabling les prevents the exploit. The vulnerability was patched in version 1.9.25. **CVE ID : CVE-2020-26264**	https://github.com/ethereum/go-ethereum/security/advisories/GHSA-r33q-22hv-j29q	A-ETH-GO_E-171220/117
Incorrect Calculation	11-Dec-20	3.5	Go Ethereum, or "Geth", is the official Golang implementation of the Ethereum protocol. In Geth from version 1.9.4 and before version 1.9.20 a consensus-vulnerability could cause a chain split,	https://github.com/ethereum/go-ethereum/security/advisories/GHSA-xw37-57qp-	A-ETH-GO_E-171220/118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			where vulnerable versions refuse to accept the canonical chain. The fix was included in the Paragade release version 1.9.20. No individual workaround patches have been made -- all users are recommended to upgrade to a newer version. **CVE ID : CVE-2020-26265**	9mm4	
express-gateway					
express-gateway_docker					
N/A	08-Dec-20	10	The official Express Gateway Docker images before 1.14.0 contain a blank password for a root user. Systems using the Express Gateway Docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access. **CVE ID : CVE-2020-29579**	N/A	A-EXP-EXPR-171220/119
F5					
nginx_controller					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	7.5	In versions 3.0.0-3.9.0, 2.0.0-2.9.0, and 1.0.1, the NGINX Controller Agent does not use absolute paths when calling system utilities. **CVE ID : CVE-2020-27730**	https://support.f5.com/csp/article/K43530108	A-F5-NGIN-171220/120
big-ip_ssl_orchestrator					
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4,	https://support.f5.com	A-F5-BIG--171220/121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break. **CVE ID : CVE-2020-5949**	/csp/article/K20984059	
big-ip_access_policy_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	6.8	On BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role. **CVE ID : CVE-2020-5948**	https://support.f5.com/csp/article/K42696541	A-F5-BIG--171220/122
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break. **CVE ID : CVE-2020-5949**	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/123
big-ip_advanced_firewall_manager					
Improper Release of Memory Before Removing Last Reference	11-Dec-20	5	In certain configurations on version 13.1.3.4, when a BIG-IP AFM HTTP security profile is applied to a virtual server and the BIG-IP system receives a request with specific characteristics, the connection is reset and the Traffic Management	https://support.f5.com/csp/article/K37960100	A-F5-BIG--171220/124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) leaks memory. **CVE ID : CVE-2020-27713**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	6.8	On BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role. **CVE ID : CVE-2020-5948**	https://support.f5.com/csp/article/K42696541	A-F5-BIG--171220/125
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break. **CVE ID : CVE-2020-5949**	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/126
Uncontrolled Resource Consumption	11-Dec-20	5	On BIG-IP 14.1.0-14.1.2.6, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role. **CVE ID : CVE-2020-5950**	https://support.f5.com/csp/article/K42696541	A-F5-BIG--171220/127
big-ip_analytics					
Improper Neutralization of Input	11-Dec-20	6.8	On BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-	https://support.f5.com/csp/article	A-F5-BIG--171220/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role. **CVE ID : CVE-2020-5948**	/K42696541	
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break. **CVE ID : CVE-2020-5949**	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/129
big-ip_application_acceleration_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	6.8	On BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role. **CVE ID : CVE-2020-5948**	https://support.f5.com/csp/article/K42696541	A-F5-BIG--171220/130
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			break. **CVE ID : CVE-2020-5949**		
big-ip_application_security_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	6.8	On BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role. **CVE ID : CVE-2020-5948**	https://support.f5.com/csp/article/K42696541	A-F5-BIG--171220/132
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break. **CVE ID : CVE-2020-5949**	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/133
big-ip_domain_name_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	6.8	On BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role.	https://support.f5.com/csp/article/K42696541	A-F5-BIG--171220/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5948		
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break. **CVE ID : CVE-2020-5949**	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/135
big-ip_fraud_protection_service					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	6.8	On BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role. **CVE ID : CVE-2020-5948**	https://support.f5.com/csp/article/K42696541	A-F5-BIG--171220/136
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break. **CVE ID : CVE-2020-5949**	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/137
big-ip_global_traffic_manager					
Improper Neutralization of Input During Web Page	11-Dec-20	6.8	On BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, undisclosed	https://support.f5.com/csp/article/K42696541	A-F5-BIG--171220/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role. **CVE ID : CVE-2020-5948**		
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break. **CVE ID : CVE-2020-5949**	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/139
big-ip_link_controller					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	6.8	On BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role. **CVE ID : CVE-2020-5948**	https://support.f5.com/csp/article/K42696541	A-F5-BIG--171220/140
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break.	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5949		
big-ip_local_traffic_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	6.8	On BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role. **CVE ID : CVE-2020-5948**	https://support.f5.com/csp/article/K42696541	A-F5-BIG--171220/142
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break. **CVE ID : CVE-2020-5949**	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/143
big-ip_policy_enforcement_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	6.8	On BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role. **CVE ID : CVE-2020-5948**	https://support.f5.com/csp/article/K42696541	A-F5-BIG--171220/144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break. **CVE ID : CVE-2020-5949**	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/145
big-ip_advanced_web_application_firewall					
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break. **CVE ID : CVE-2020-5949**	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/146
big-ip_ddos_hybrid_defender					
N/A	11-Dec-20	5	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break. **CVE ID : CVE-2020-5949**	https://support.f5.com/csp/article/K20984059	A-F5-BIG--171220/147
fastadmin					
fastadmin					
Improper Control of Generation of Code ('Code Injection')	10-Dec-20	6.5	The member center function in fastadmin V1.0.0.20200506_beta is vulnerable to a Server-Side Template Injection (SSTI) vulnerability. **CVE ID : CVE-2020-25967**	N/A	A-FAS-FAST-171220/148
Fasterxml					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jackson-databind					
Improper Restriction of XML External Entity Reference ('XXE')	03-Dec-20	5	A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity. **CVE ID : CVE-2020-25649**	N/A	A-FAS-JACK-171220/149
Fedoraproject					
fedora_extra_packages_for_enterprise_linux					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-20	4.3	A flaw was found in the check_chunk_name() function of pngcheck-2.4.0. An attacker able to pass a malicious file to be processed by pngcheck could cause a temporary denial of service, posing a low risk to application availability. **CVE ID : CVE-2020-27818**	https://bugzilla.redhat.com/show_bug.cgi?id=1902011	A-FED-FEDO-171220/150
Flexense					
dupscout					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Dec-20	10	A buffer overflow in the web server of Flexense DupScout Enterprise 10.0.18 allows a remote anonymous attacker to execute code as SYSTEM by overflowing the sid parameter via a GET /settings&sid= attack. **CVE ID : CVE-2020-29659**	N/A	A-FLE-DUPS-171220/151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fnet_project					
fnet					
Out-of-bounds Read	11-Dec-20	6.4	An issue was discovered in FNET through 4.6.4. The code for processing resource records in mDNS queries doesn't check for proper '\0' termination of the resource record name string, leading to an out-of-bounds read, and potentially causing information leak or Denial-or-Service. **CVE ID : CVE-2020-24383**	N/A	A-FNE-FNET-171220/152
frappe					
frappe					
N/A	11-Dec-20	5	In two-factor authentication, the system also sending 2fa secret key in response, which enables an intruder to breach the 2fa security. **CVE ID : CVE-2020-27508**	N/A	A-FRA-FRAP-171220/153
Improper Input Validation	11-Dec-20	5	Frappe Framework 12 and 13 does not properly validate the HTTP method for the frappe.client API. **CVE ID : CVE-2020-35175**	N/A	A-FRA-FRAP-171220/154
Freedesktop					
poppler					
Access of Uninitialized Pointer	03-Dec-20	5	A flaw was found in Poppler in the way certain PDF files were converted into HTML. A remote attacker could exploit this flaw by providing a malicious PDF file that, when processed by	N/A	A-FRE-POPP-171220/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the 'pdftohtml' program, would crash the application causing a denial of service. **CVE ID : CVE-2020-27778**		
Getkirby					
Kirby					
Origin Validation Error	08-Dec-20	4.3	Kirby is a CMS. In Kirby CMS (getkirby/cms) before version 3.3.6, and Kirby Panel before version 2.5.14 there is a vulnerability in which the admin panel may be accessed if hosted on a .dev domain. In order to protect new installations on public servers that don't have an admin account for the Panel yet, we block account registration there by default. This is a security feature, which we implemented years ago in Kirby 2. It helps to avoid that you forget registering your first admin account on a public server. In this case – without our security block – someone else might theoretically be able to find your site, find out it's running on Kirby, find the Panel and then register the account first. It's an unlikely situation, but it's still a certain risk. To be able to register the first Panel account on a public server, you have to enforce the installer via a config setting.	https://github.com/getkirby/kirby/security/advisories/GHSA-2ccx-2gf3-8xvv	A-GET-KIRB-171220/156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This helps to push all users to the best practice of registering your first Panel account on your local machine and upload it together with the rest of the site. This installation block implementation in Kirby versions before 3.3.6 still assumed that .dev domains are local domains, which is no longer true. In the meantime, those domains became publicly available. This means that our installation block is no longer working as expected if you use a .dev domain for your Kirby site. Additionally the local installation check may also fail if your site is behind a reverse proxy. You are only affected if you use a .dev domain or your site is behind a reverse proxy and you have not yet registered your first Panel account on the public server and someone finds your site and tries to login at `yourdomain.dev/panel` before you register your first account. You are not affected if you have already created one or multiple Panel accounts (no matter if on a .dev domain or behind a reverse proxy). The problem has been patched in Kirby 3.3.6. Please upgrade to this		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or a later version to fix the vulnerability. **CVE ID : CVE-2020-26253**		
Unrestricted Upload of File with Dangerous Type	08-Dec-20	6.5	Kirby is a CMS. In Kirby CMS (getkirby/cms) before version 3.4.5, and Kirby Panel before version 2.5.14 , an editor with full access to the Kirby Panel can upload a PHP .phar file and execute it on the server. This vulnerability is critical if you might have potential attackers in your group of authenticated Panel users, as they can gain access to the server with such a Phar file. Visitors without Panel access *cannot* use this attack vector. The problem has been patched in Kirby 2.5.14 and Kirby 3.4.5. Please update to one of these or a later version to fix the vulnerability. Note: Kirby 2 reaches end of life on December 31, 2020. We therefore recommend to upgrade your Kirby 2 sites to Kirby 3. If you cannot upgrade, we still recommend to update to Kirby 2.5.14. **CVE ID : CVE-2020-26255**	https://github.com/getkirby/kirby/security/advisories/GHSA-g3h8-cg9x-47qw	A-GET-KIRB-171220/157
panel					
Origin Validation Error	08-Dec-20	4.3	Kirby is a CMS. In Kirby CMS (getkirby/cms) before version 3.3.6, and Kirby Panel before version 2.5.14 there is a vulnerability in	https://github.com/getkirby/kirby/security/advisories/G	A-GET-PANE-171220/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which the admin panel may be accessed if hosted on a .dev domain. In order to protect new installations on public servers that don't have an admin account for the Panel yet, we block account registration there by default. This is a security feature, which we implemented years ago in Kirby 2. It helps to avoid that you forget registering your first admin account on a public server. In this case – without our security block – someone else might theoretically be able to find your site, find out it's running on Kirby, find the Panel and then register the account first. It's an unlikely situation, but it's still a certain risk. To be able to register the first Panel account on a public server, you have to enforce the installer via a config setting. This helps to push all users to the best practice of registering your first Panel account on your local machine and upload it together with the rest of the site. This installation block implementation in Kirby versions before 3.3.6 still assumed that .dev domains are local domains, which is no longer true. In the	HSA-2ccx-2gf3-8xvv	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			meantime, those domains became publicly available. This means that our installation block is no longer working as expected if you use a .dev domain for your Kirby site. Additionally the local installation check may also fail if your site is behind a reverse proxy. You are only affected if you use a .dev domain or your site is behind a reverse proxy and you have not yet registered your first Panel account on the public server and someone finds your site and tries to login at `yourdomain.dev/panel` before you register your first account. You are not affected if you have already created one or multiple Panel accounts (no matter if on a .dev domain or behind a reverse proxy). The problem has been patched in Kirby 3.3.6. Please upgrade to this or a later version to fix the vulnerability. **CVE ID : CVE-2020-26253**		
Unrestricted Upload of File with Dangerous Type	08-Dec-20	6.5	Kirby is a CMS. In Kirby CMS (getkirby/cms) before version 3.4.5, and Kirby Panel before version 2.5.14 , an editor with full access to the Kirby Panel can upload a PHP .phar file and execute it on the server. This vulnerability is critical if you	https://github.com/getkirby/kirby/security/advisories/GHSA-g3h8-cg9x-47qw	A-GET-PANE-171220/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			might have potential attackers in your group of authenticated Panel users, as they can gain access to the server with such a Phar file. Visitors without Panel access *cannot* use this attack vector. The problem has been patched in Kirby 2.5.14 and Kirby 3.4.5. Please update to one of these or a later version to fix the vulnerability. Note: Kirby 2 reaches end of life on December 31, 2020. We therefore recommend to upgrade your Kirby 2 sites to Kirby 3. If you cannot upgrade, we still recommend to update to Kirby 2.5.14. **CVE ID : CVE-2020-26255**		
Gitlab					
gitlab					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	3.5	A XSS vulnerability exists in Gitlab CE/EE from 12.4 before 13.4.7, 13.5 before 13.5.5, and 13.6 before 13.6.2 that allows an attacker to perform cross-site scripting to other users via importing a malicious project **CVE ID : CVE-2020-26407**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26407.json	A-GIT-GITL-171220/160
Information Exposure	11-Dec-20	5	A limited information disclosure vulnerability exists in Gitlab CE/EE from >= 12.2 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to	https://gitlab.com/gitlab-org/cves/-/blob/mast	A-GIT-GITL-171220/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<13.6.2 that allows an attacker to view limited information in user's private profile **CVE ID : CVE-2020-26408**	er/2020/CVE-2020-26408.json	
Improper Input Validation	11-Dec-20	4	A DOS vulnerability exists in Gitlab CE/EE >=10.3, <13.4.7,>=13.5, <13.5.5,>=13.6, <13.6.2 that allows an attacker to trigger uncontrolled resource by bypassing input validation in markdown fields. **CVE ID : CVE-2020-26409**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26409.json	A-GIT-GITL-171220/162
Improper Resource Shutdown or Release	11-Dec-20	4	A potential DOS vulnerability was discovered in all versions of Gitlab starting from 13.4.x (>=13.4 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to <13.6.2). Using a specific query name for a project search can cause statement timeouts that can lead to a potential DOS if abused. **CVE ID : CVE-2020-26411**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26411.json	A-GIT-GITL-171220/163
Information Exposure	11-Dec-20	4	Removed group members were able to use the To-Do functionality to retrieve updated information on confidential epics starting in GitLab EE 13.2 before 13.6.2. **CVE ID : CVE-2020-26412**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26412.json	A-GIT-GITL-171220/164
Information Exposure	11-Dec-20	5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.4 before 13.6.2.	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-171220/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information disclosure via GraphQL results in user email being unexpectedly visible. **CVE ID : CVE-2020-26413**	/blob/master/2020/CVE-2020-26413.json	
Information Exposure	11-Dec-20	4	Information about the starred projects for private user profiles was exposed via the GraphQL API starting from 12.2 via the REST API. This affects GitLab >=12.2 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to <13.6.2. **CVE ID : CVE-2020-26415**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26415.json	A-GIT-GITL-171220/166
Information Exposure	11-Dec-20	2.1	Information disclosure in Advanced Search component of GitLab EE starting from 8.4 results in exposure of search terms via Rails logs. This affects versions >=8.4 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to <13.6.2. **CVE ID : CVE-2020-26416**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26416.json	A-GIT-GITL-171220/167
Information Exposure	11-Dec-20	5	Information disclosure via GraphQL in GitLab CE/EE 13.1 and later exposes private group and project membership. This affects versions >=13.6 to <13.6.2, >=13.5 to <13.5.5, and >=13.1 to <13.4.7. **CVE ID : CVE-2020-26417**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26417.json	A-GIT-GITL-171220/168
Authorization Bypass Through User-Controlled	11-Dec-20	4	An issue was discovered in Gitlab CE/EE versions >= 13.1 to <13.4.7, >= 13.5 to <13.5.5, and >= 13.6 to <13.6.2 allowed an unauthorized user to access	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/C	A-GIT-GITL-171220/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Key			the user list corresponding to a feature flag in a project. **CVE ID : CVE-2020-13357**	VE-2020-13357.json	
GNU					
glibc					
Reachable Assertion	04-Dec-20	5	The iconv function in the GNU C Library (aka glibc or libc6) 2.30 to 2.32, when converting UCS4 text containing an irreversible character, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service. **CVE ID : CVE-2020-29562**	N/A	A-GNU-GLIB-171220/170
Out-of-bounds Write	06-Dec-20	5	sysdeps/i386/ldbl2mpn.c in the GNU C Library (aka glibc or libc6) before 2.23 on x86 targets has a stack-based buffer overflow if the input to any of the printf family of functions is an 80-bit long double with a non-canonical bit pattern, as seen when passing a \x00\x04\x00\x00\x00\x00\x00\x00\x00\x04 value to sprintf. NOTE: the issue does not affect glibc by default in 2016 or later (i.e., 2.23 or later) because of commits made in 2015 for inlining of C99 math functions through use of GCC built-ins. In other words, the reference to 2.23 is intentional despite the	N/A	A-GNU-GLIB-171220/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mention of "Fixed for glibc 2.33" in the 26649 reference. **CVE ID : CVE-2020-29573**		
binutils					
Double Free	09-Dec-20	4.3	A double free vulnerability exists in the Binary File Descriptor (BFD) (aka libbrd) in GNU Binutils 2.34 in the process_symbol_table, as demonstrated in readelf, via a crafted file. **CVE ID : CVE-2020-16590**	N/A	A-GNU-BINU-171220/172
Out-of-bounds Read	09-Dec-20	4.3	A Denial of Service vulnerability exists in the Binary File Descriptor (BFD) in GNU Binutils 2.34 due to an invalid read in process_symbol_table, as demonstrated in readeif. **CVE ID : CVE-2020-16591**	N/A	A-GNU-BINU-171220/173
Use After Free	09-Dec-20	4.3	A use after free issue exists in the Binary File Descriptor (BFD) library (aka libbfd) in GNU Binutils 2.34 in bfd_hash_lookup, as demonstrated in nm-new, that can cause a denial of service via a crafted file. **CVE ID : CVE-2020-16592**	N/A	A-GNU-BINU-171220/174
NULL Pointer Dereference	09-Dec-20	4.3	A Null Pointer Dereference vulnerability exists in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.34, in scan_unit_for_symbols, as demonstrated in addr2line,	N/A	A-GNU-BINU-171220/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that can cause a denial of service via a crafted file. **CVE ID : CVE-2020-16593**		
NULL Pointer Dereference	09-Dec-20	4.3	A Null Pointer Dereference vulnerability exists in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.34, in debug_get_real_type, as demonstrated in objdump, that can cause a denial of service via a crafted file. **CVE ID : CVE-2020-16598**	N/A	A-GNU-BINU-171220/176
NULL Pointer Dereference	09-Dec-20	4.3	A Null Pointer Dereference vulnerability exists in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.34, in _bfd_elf_get_symbol_version_string, as demonstrated in nm-new, that can cause a denial of service via a crafted file. **CVE ID : CVE-2020-16599**	N/A	A-GNU-BINU-171220/177
Google					
tensorflow					
Use of Uninitialized Resource	10-Dec-20	4.6	In affected versions of TensorFlow under certain cases a saved model can trigger use of uninitialized values during code execution. This is caused by having tensor buffers be filled with the default value of the type but forgetting to default initialize the	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qhxx-j73r-qpm2	A-GOO-TENS-171220/178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			quantized floating point types in Eigen. This is fixed in versions 1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, and 2.4.0. **CVE ID : CVE-2020-26266**		
N/A	10-Dec-20	3.6	In affected versions of TensorFlow the tf.raw_ops.ImmutableConst operation returns a constant tensor created from a memory mapped file which is assumed immutable. However, if the type of the tensor is not an integral type, the operation crashes the Python interpreter as it tries to write to the memory area. If the file is too small, TensorFlow properly returns an error as the memory area has fewer bytes than what is needed for the tensor it creates. However, as soon as there are enough bytes, the above snippet causes a segmentation fault. This is because the allocator used to return the buffer data is not marked as returning an opaque handle since the needed virtual method is not overridden. This is fixed in versions 1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, and 2.4.0. **CVE ID : CVE-2020-26268**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-hhvc-g5hv-48c6	A-GOO-TENS-171220/179
Improper Input Validation	10-Dec-20	2.1	In affected versions of TensorFlow running an LSTM/GRU model where the	https://github.com/tensorflow/ten	A-GOO-TENS-171220/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			LSTM/GRU layer receives an input with zero-length results in a CHECK failure when using the CUDA backend. This can result in a query-of-death vulnerability, via denial of service, if users can control the input to the layer. This is fixed in versions 1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, and 2.4.0. **CVE ID : CVE-2020-26270**	sorflow/security/advisories/GHSA-m648-33qf-v3gp	
Use of Uninitialized Resource	10-Dec-20	2.1	In affected versions of TensorFlow under certain cases, loading a saved model can result in accessing uninitialized memory while building the computation graph. The MakeEdge function creates an edge between one output tensor of the src node (given by output_index) and the input slot of the dst node (given by input_index). This is only possible if the types of the tensors on both sides coincide, so the function begins by obtaining the corresponding DataType values and comparing these for equality. However, there is no check that the indices point to inside of the arrays they index into. Thus, this can result in accessing data out of bounds of the corresponding heap allocated arrays. In most scenarios, this can manifest	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-q263-fvxm-m5mw	A-GOO-TENS-171220/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as unitialized data access, but if the index points far away from the boundaries of the arrays this can be used to leak addresses from the library. This is fixed in versions 1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, and 2.4.0. **CVE ID : CVE-2020-26271**		
gorillatoolkit					
websocket					
Integer Overflow or Wraparound	02-Dec-20	5	An integer overflow vulnerability exists with the length of websocket frames received via a websocket connection. An attacker would use this flaw to cause a denial of service attack on an HTTP Server allowing websocket connections. **CVE ID : CVE-2020-27813**	N/A	A-GOR-WEBS-171220/182
gym_management_system_project					
gym_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-20	7.5	An SQL injection vulnerability was discovered in Gym Management System In manage_user.php file, GET parameter 'id' is vulnerable. **CVE ID : CVE-2020-29288**	N/A	A-GYM-GYM_-171220/183
hashicorp					
go-slug					
Improper Link Resolution	03-Dec-20	5	HashiCorp go-slug up to 0.4.3 did not fully protect against Zip Slip attacks while	N/A	A-HAS-GO-S-171220/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Before File Access ('Link Following')			unpacking tar archives, and protections could be bypassed with specific constructions of multiple symlinks. Fixed in 0.5.0. **CVE ID : CVE-2020-29529**		
consul					
N/A	08-Dec-20	10	The official Consul Docker images 0.7.1 through 1.4.2 contain a blank password for a root user. System using the Consul Docker container deployed by affected versions of the Docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-29564**	N/A	A-HAS-CONS-171220/185
Haxx					
curl					
Out-of-bounds Write	14-Dec-20	5	curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard match parsing. **CVE ID : CVE-2020-8285**	N/A	A-HAX-CURL-171220/186
Improper Certificate Validation	14-Dec-20	5	curl 7.41.0 through 7.73.0 is vulnerable to an improper check for certificate revocation due to insufficient verification of the OCSP response. **CVE ID : CVE-2020-8286**	N/A	A-HAX-CURL-171220/187
Information Exposure	14-Dec-20	5	curl 7.62.0 through 7.70.0 is vulnerable to an information disclosure vulnerability that can lead to a partial	N/A	A-HAX-CURL-171220/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			password being leaked over the network and to the DNS server(s). **CVE ID : CVE-2020-8169**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	14-Dec-20	4.6	curl 7.20.0 through 7.70.0 is vulnerable to improper restriction of names for files and other resources that can lead too overwriting a local file when the -J flag is used. **CVE ID : CVE-2020-8177**	N/A	A-HAX-CURL-171220/189
hcltech					
domino					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-20	10	HCL Domino is susceptible to a Buffer Overflow vulnerability in DXL due to improper validation of user input. A successful exploit could enable an attacker to crash Domino or execute attacker-controlled code on the server system. **CVE ID : CVE-2020-14260**	N/A	A-HCL-DOMI-171220/190
Improper Authentication	01-Dec-20	5	HCL Domino is susceptible to a lockout policy bypass vulnerability in the ID Vault service. An unauthenticated attacker could use this vulnerability to mount a brute force attack against the ID Vault service. **CVE ID : CVE-2020-4128**	N/A	A-HCL-DOMI-171220/191
hcl_inotes					
Information Exposure	01-Dec-20	4.3	HCL iNotes is susceptible to a sensitive cookie exposure	N/A	A-HCL-HCL_-171220/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This can allow an unauthenticated remote attacker to capture the cookie by intercepting its transmission within an http session. Fixes are available in HCL Domino and iNotes versions 10.0.1 FP6 and 11.0.1 FP2 and later. **CVE ID : CVE-2020-4126**		
hcl_domino					
N/A	01-Dec-20	5	HCL Domino is susceptible to a lockout policy bypass vulnerability in the LDAP service. An unauthenticated attacker could use this vulnerability to mount a brute force attack against the LDAP service. Fixes are available in HCL Domino versions 9.0.1 FP10 IF6, 10.0.1 FP6 and 11.0.1 FP1 and later. **CVE ID : CVE-2020-4129**	N/A	A-HCL-HCL_-171220/193
notes					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-20	7.2	HCL Notes is susceptible to a Buffer Overflow vulnerability in DXL due to improper validation of user input. A successful exploit could enable an attacker to crash Notes or execute attacker-controlled code on the client system. **CVE ID : CVE-2020-4102**	N/A	A-HCL-NOTE-171220/194
Hibernate					
hibernate_orm					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-20	5.8	A flaw was found in hibernate-core in versions prior to and including 5.4.23.Final. A SQL injection in the implementation of the JPA Criteria API can permit unsanitized literals when a literal is used in the SQL comments of the query. This flaw could allow an attacker to access unauthorized information or possibly conduct further attacks. The highest threat from this vulnerability is to data confidentiality and integrity. **CVE ID : CVE-2020-25638**	N/A	A-HIB-HIBE-171220/195
HP					
edgeline_infrastructure_manager					
Improper Authentication	02-Dec-20	10	A security vulnerability has been identified in the HPE Edgeline Infrastructure Manager, also known as HPE Edgeline Infrastructure Management Software. The vulnerability could be remotely exploited to bypass remote authentication leading to execution of arbitrary commands, gaining privileged access, causing denial of service, and changing the configuration. **CVE ID : CVE-2020-7199**	N/A	A-HP-EDGE-171220/196
Huawei					
fusioncompute					
Improper Privilege	01-Dec-20	7.2	FusionCompute versions 6.3.0, 6.3.1, 6.5.0, 6.5.1 and	N/A	A-HUA-FUSI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			8.0.0 have a privilege escalation vulnerability. Due to improper privilege management, an attacker with common privilege may access some specific files and get the administrator privilege in the affected products. Successful exploit will cause privilege escalation. **CVE ID : CVE-2020-9114**		171220/197
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Dec-20	6.5	Huawei FusionCompute versions 6.5.1 and 8.0.0 have a command injection vulnerability. An authenticated, remote attacker can craft specific request to exploit this vulnerability. Due to insufficient verification, this could be exploited to cause the attackers to obtain higher privilege. **CVE ID : CVE-2020-9116**	N/A	A-HUA-FUSI-171220/198
manageone					
Improper Input Validation	01-Dec-20	9	ManageOne versions 6.5.1.1.B010, 6.5.1.1.B020, 6.5.1.1.B030, 6.5.1.1.B040, ,6.5.1.1.B050, 8.0.0 and 8.0.1 have a command injection vulnerability. An attacker with high privileges may exploit this vulnerability through some operations on the plug-in component. Due to insufficient input validation of some parameters, the attacker can	N/A	A-HUA-MANA-171220/199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability to inject commands to the target device. **CVE ID : CVE-2020-9115**		
i18n_project					
i18n					
N/A	11-Dec-20	5	This affects the package i18n before 2.1.15. Vulnerability arises out of insufficient handling of erroneous language tags in src/i18n/Concrete/TextLocalizer.cs and src/i18n/LocalizedApplication.cs. **CVE ID : CVE-2020-7791**	N/A	A-I18-I18N-171220/200
IBM					
resilient_security_orchestration_automation_and_response					
Improper Input Validation	11-Dec-20	9	IBM Resilient SOAR V38.0 could allow a remote attacker to execute arbitrary code on the system, caused by formula injection due to improper input validation. **CVE ID : CVE-2020-4633**	https://www.ibm.com/support/pages/node/6380884	A-IBM-RESI-171220/201
idreamsoft					
icms					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Dec-20	10	iCMS 7 attackers to execute arbitrary OS commands via shell metacharacters in the DB_PREFIX parameter to install/install.php. **CVE ID : CVE-2020-19142**	N/A	A-IDR-ICMS-171220/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Dec-20	10	iCMS 7.0.14 attackers to execute arbitrary OS commands via shell metacharacters in the DB_NAME parameter to install/install.php. **CVE ID : CVE-2020-19527**	N/A	A-IDR-ICMS-171220/203
Igniterealtime					
openfire					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	3.5	Ignite Realtime Openfire 4.6.0 has plugins/bookmarks/create-bookmark.jsp Stored XSS. **CVE ID : CVE-2020-35127**	N/A	A-IGN-OPEN-171220/204
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-20	4.3	Ignite Realtime Openfire 4.6.0 has plugins/clientcontrol/spark-form.jsp Reflective XSS. **CVE ID : CVE-2020-35200**	N/A	A-IGN-OPEN-171220/205
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-20	3.5	Ignite Realtime Openfire 4.6.0 has create-bookmark.jsp users Stored XSS. **CVE ID : CVE-2020-35201**	N/A	A-IGN-OPEN-171220/206
Improper Neutralization of Input	12-Dec-20	3.5	Ignite Realtime Openfire 4.6.0 has plugins/dbaccess/db-	N/A	A-IGN-OPEN-171220/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			access.jsp sql Stored XSS. **CVE ID : CVE-2020-35202**		
Imagemagick					
imagemagick					
Improper Release of Memory Before Removing Last Reference	08-Dec-20	4.3	in SetImageExtent() of /MagickCore/image.c, an incorrect image depth size can cause a memory leak because the code which checks for the proper image depth size does not reset the size in the event there is an invalid size. The patch resets the depth to a proper size before throwing an exception. The memory leak can be triggered by a crafted input file that is processed by ImageMagick and could cause an impact to application reliability, such as denial of service. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27755**	N/A	A-IMA-IMAG-171220/208
Divide By Zero	08-Dec-20	4.3	In ParseMetaGeometry() of MagickCore/geometry.c, image height and width calculations can lead to divide-by-zero conditions which also lead to undefined behavior. This flaw can be triggered by a crafted input file processed by ImageMagick and could impact application	N/A	A-IMA-IMAG-171220/209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			availability. The patch uses multiplication in addition to the function `PerceptibleReciprocal()` in order to prevent such divide-by-zero conditions. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27756**		
Integer Overflow or Wraparound	08-Dec-20	4.3	A floating point math calculation in ScaleAnyToQuantum() of /MagickCore/quantum-private.h could lead to undefined behavior in the form of a value outside the range of type unsigned long long. The flaw could be triggered by a crafted input file under certain conditions when it is processed by ImageMagick. Red Hat Product Security marked this as Low because although it could potentially lead to an impact to application availability, no specific impact was shown in this case. This flaw affects ImageMagick versions prior to 7.0.8-68. **CVE ID : CVE-2020-27757**	N/A	A-IMA-IMAG-171220/210
Integer Overflow or Wraparound	08-Dec-20	4.3	A flaw was found in ImageMagick in coders/txt.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior	N/A	A-IMA-IMAG-171220/211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the form of values outside the range of type `unsigned long long`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.8-68. **CVE ID : CVE-2020-27758**		
Integer Overflow or Wraparound	03-Dec-20	4.3	In IntensityCompare() of /MagickCore/quantize.c, a double value was being casted to int and returned, which in some cases caused a value outside the range of type `int` to be returned. The flaw could be triggered by a crafted input file under certain conditions when processed by ImageMagick. Red Hat Product Security marked this as Low severity because although it could potentially lead to an impact to application availability, no specific impact was shown in this case. This flaw affects ImageMagick versions prior to 7.0.8-68. **CVE ID : CVE-2020-27759**	N/A	A-IMA-IMAG-171220/212
Divide By Zero	03-Dec-20	4.3	In `GammaImage()` of /MagickCore/enhance.c, depending on the `gamma` value, it's possible to trigger a divide-by-zero condition when a crafted input file is processed by ImageMagick.	N/A	A-IMA-IMAG-171220/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to an impact to application availability. The patch uses the `PerceptibleReciprocal()` to prevent the divide-by-zero from occurring. This flaw affects ImageMagick versions prior to ImageMagick 7.0.8-68. **CVE ID : CVE-2020-27760**		
Integer Overflow or Wraparound	03-Dec-20	4.3	WritePALMImage() in /coders/palm.c used size_t casts in several areas of a calculation which could lead to values outside the range of representable type `unsigned long` undefined behavior when a crafted input file was processed by ImageMagick. The patch casts to `ssize_t` instead to avoid this issue. Red Hat Product Security marked the Severity as Low because although it could potentially lead to an impact to application availability, no specific impact was shown in this case. This flaw affects ImageMagick versions prior to ImageMagick 7.0.9-0. **CVE ID : CVE-2020-27761**	N/A	A-IMA-IMAG-171220/214
Integer Overflow or Wraparound	03-Dec-20	4.3	A flaw was found in ImageMagick in coders/hdr.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the	N/A	A-IMA-IMAG-171220/215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			form of values outside the range of type `unsigned char`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to ImageMagick 7.0.8-68. **CVE ID : CVE-2020-27762**		
Divide By Zero	03-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/resize.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.8-68. **CVE ID : CVE-2020-27763**	N/A	A-IMA-IMAG-171220/216
Integer Overflow or Wraparound	03-Dec-20	4.3	In /MagickCore/statistic.c, there are several areas in ApplyEvaluateOperator() where a size_t cast should have been a ssize_t cast, which causes out-of-range values under some circumstances when a crafted input file is processed by ImageMagick.	N/A	A-IMA-IMAG-171220/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Red Hat Product Security marked this as Low severity because although it could potentially lead to an impact to application availability, no specific impact was shown in this case. This flaw affects ImageMagick versions prior to 6.9.10-69. **CVE ID : CVE-2020-27764**		
Divide By Zero	04-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/segment.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27765**	N/A	A-IMA-IMAG-171220/218
Integer Overflow or Wraparound	04-Dec-20	6.8	A flaw was found in ImageMagick in MagickCore/statistic.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned long`. This would most likely lead to an impact to application availability, but	N/A	A-IMA-IMAG-171220/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.8-69. **CVE ID : CVE-2020-27766**		
Integer Overflow or Wraparound	04-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/quantum.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of types `float` and `unsigned char`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27767**	N/A	A-IMA-IMAG-171220/220
Integer Overflow or Wraparound	04-Dec-20	4.3	Due to a missing check for 0 value of `replace_extent`, it is possible for offset `p` to overflow in SubstituteString(), causing potential impact to application availability. This could be triggered by a crafted input file that is processed by ImageMagick. This flaw affects ImageMagick versions prior to 7.0.8-68. **CVE ID : CVE-2020-27770**	N/A	A-IMA-IMAG-171220/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Dec-20	4.3	In RestoreMSCWarning() of /coders/pdf.c there are several areas where calls to GetPixelIndex() could result in values outside the range of representable for the unsigned char type. The patch casts the return value of GetPixelIndex() to ssize_t type to avoid this bug. This undefined behavior could be triggered when ImageMagick processes a crafted pdf file. Red Hat Product Security marked this as Low severity because although it could potentially lead to an impact to application availability, no specific impact was demonstrated in this case. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27771**	N/A	A-IMA-IMAG-171220/222
Integer Overflow or Wraparound	04-Dec-20	4.3	A flaw was found in ImageMagick in coders/bmp.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned int`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This	N/A	A-IMA-IMAG-171220/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27772**		
Divide By Zero	04-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/gem-private.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned char` or division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27773**	N/A	A-IMA-IMAG-171220/224
Integer Overflow or Wraparound	04-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/statistic.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of a too large shift for 64-bit type `ssize_t`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0.	N/A	A-IMA-IMAG-171220/225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-27774		
Integer Overflow or Wraparound	04-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/quantum.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type unsigned char. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27775**	N/A	A-IMA-IMAG-171220/226
Integer Overflow or Wraparound	04-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/statistic.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type unsigned long. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27776**	N/A	A-IMA-IMAG-171220/227
Use After	08-Dec-20	4.3	A call to ConformPixelInfo() in the	N/A	A-IMA-IMAG-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			SetImageAlphaChannel() routine of /MagickCore/channel.c caused a subsequent heap-use-after-free or heap-buffer-overflow READ when GetPixelRed() or GetPixelBlue() was called. This could occur if an attacker is able to submit a malicious image file to be processed by ImageMagick and could lead to denial of service. It likely would not lead to anything further because the memory is used as pixel data and not e.g. a function pointer. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-25663**		171220/228
Out-of-bounds Write	08-Dec-20	5.8	In WriteOnePNGImage() of the PNG coder at coders/png.c, an improper call to AcquireVirtualMemory() and memset() allows for an out-of-bounds write later when PopShortPixel() from MagickCore/quantum-private.h is called. The patch fixes the calls by adding 256 to rowbytes. An attacker who is able to supply a specially crafted image could affect availability with a low impact to data integrity. This flaw affects ImageMagick versions prior to 6.9.10-68	N/A	A-IMA-IMAG-171220/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 7.0.8-68. **CVE ID : CVE-2020-25664**		
Out-of-bounds Read	08-Dec-20	4.3	The PALM image coder at coders/palm.c makes an improper call to AcquireQuantumMemory() in routine WritePALMImage() because it needs to be offset by 256. This can cause a out-of-bounds read later on in the routine. The patch adds 256 to bytes_per_row in the call to AcquireQuantumMemory(). This could cause impact to reliability. This flaw affects ImageMagick versions prior to 7.0.8-68. **CVE ID : CVE-2020-25665**	N/A	A-IMA-IMAG-171220/230
Integer Overflow or Wraparound	08-Dec-20	4.3	There are 4 places in HistogramCompare() in MagickCore/histogram.c where an integer overflow is possible during simple math calculations. This occurs in the rgb values and `count` value for a color. The patch uses casts to `ssize_t` type for these calculations, instead of `int`. This flaw could impact application reliability in the event that ImageMagick processes a crafted input file. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-25666**	N/A	A-IMA-IMAG-171220/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Dec-20	4.3	TIFFGetProfiles() in /coders/tiff.c calls strstr() which causes a large out-of-bounds read when it searches for `"dc:format=\"image/dng\"` within `profile` due to improper string handling, when a crafted input file is provided to ImageMagick. The patch uses a StringInfo type instead of a raw C string to remedy this. This could cause an impact to availability of the application. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-25667**	N/A	A-IMA-IMAG-171220/232
Out-of-bounds Read	08-Dec-20	4.3	WriteOnePNGImage() from coders/png.c (the PNG coder) has a for loop with an improper exit condition that can allow an out-of-bounds READ via heap-buffer-overflow. This occurs because it is possible for the colormap to have less than 256 valid values but the loop condition will loop 256 times, attempting to pass invalid colormap data to the event logger. The patch replaces the hardcoded 256 value with a call to MagickMin() to ensure the proper value is used. This could impact application availability when a specially crafted input file is	N/A	A-IMA-IMAG-171220/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processed by ImageMagick. This flaw affects ImageMagick versions prior to 7.0.8-68. **CVE ID : CVE-2020-25674**		
Integer Overflow or Wraparound	08-Dec-20	4.3	In the CropImage() and CropImageToTiles() routines of MagickCore/transform.c, rounding calculations performed on unconstrained pixel offsets was causing undefined behavior in the form of integer overflow and out-of-range values as reported by UndefinedBehaviorSanitizer. Such issues could cause a negative impact to application availability or other problems related to undefined behavior, in cases where ImageMagick processes untrusted input data. The upstream patch introduces functionality to constrain the pixel offsets and prevent these issues. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-25675**	N/A	A-IMA-IMAG-171220/234
Integer Overflow or Wraparound	08-Dec-20	4.3	In CatromWeights(), MeshInterpolate(), InterpolatePixelChannel(), InterpolatePixelChannels(), and InterpolatePixelInfo(), which are all functions in /MagickCore/pixel.c, there	N/A	A-IMA-IMAG-171220/235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			were multiple unconstrained pixel offset calculations which were being used with the floor() function. These calculations produced undefined behavior in the form of out-of-range and integer overflows, as identified by UndefinedBehaviorSanitizer. These instances of undefined behavior could be triggered by an attacker who is able to supply a crafted input file to be processed by ImageMagick. These issues could impact application availability or potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-25676**		
Divide By Zero	08-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/colorspace-private.h and MagickCore/quantum.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned char` and math division by zero. This would most likely lead to an impact to application availability, but could potentially cause other	N/A	A-IMA-IMAG-171220/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.8-68. **CVE ID : CVE-2020-27750**		
Integer Overflow or Wraparound	08-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/quantum-export.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned long long` as well as a shift exponent that is too large for 64-bit type. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27751**	N/A	A-IMA-IMAG-171220/237
Out-of-bounds Write	08-Dec-20	5.8	A flaw was found in ImageMagick in MagickCore/quantum-private.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger a heap buffer overflow. This would most likely lead to an impact to application availability, but could potentially lead to an impact to data integrity as well. This flaw affects	N/A	A-IMA-IMAG-171220/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27752**		
Improper Release of Memory Before Removing Last Reference	08-Dec-20	4.3	There are several memory leaks in the MIFF coder in /coders/miff.c due to improper image depth values, which can be triggered by a specially crafted input file. These leaks could potentially lead to an impact to application availability or cause a denial of service. It was originally reported that the issues were in `AcquireMagickMemory()` because that is where LeakSanitizer detected the leaks, but the patch resolves issues in the MIFF coder, which incorrectly handles data being passed to `AcquireMagickMemory()`. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27753**	N/A	A-IMA-IMAG-171220/239
Integer Overflow or Wraparound	08-Dec-20	4.3	In IntensityCompare() of /magick/quantize.c, there are calls to PixelPacketIntensity() which could return overflowed values to the caller when ImageMagick processes a crafted input file. To mitigate this, the patch introduces and uses the ConstrainPixelIntensity()	N/A	A-IMA-IMAG-171220/240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function, which forces the pixel intensities to be within the proper bounds in the event of an overflow. This flaw affects ImageMagick versions prior to 6.9.10-69 and 7.0.8-69. **CVE ID : CVE-2020-27754**		
XML Injection (aka Blind XPath Injection)	07-Dec-20	7.5	ImageMagick before 6.9.11-40 and 7.x before 7.0.10-40 mishandles the -authenticate option, which allows setting a password for password-protected PDF files. The user-controlled password was not properly escaped/sanitized and it was therefore possible to inject additional shell commands via coders/pdf.c. **CVE ID : CVE-2020-29599**	N/A	A-IMA-IMAG-171220/241
incomcms_project					
incomcms					
Unrestricted Upload of File with Dangerous Type	07-Dec-20	7.5	IncomCMS 2.0 has a modules/uploader/showcase/script.php insecure file upload vulnerability. This vulnerability allows unauthenticated attackers to upload files into the server. **CVE ID : CVE-2020-29597**	N/A	A-INC-INCO-171220/242
infinispan					
infinispan					
Improper Privilege Management	03-Dec-20	4.9	A flaw was found in infinispan 10 REST API, where authorization permissions are not checked	N/A	A-INF-INFI-171220/243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while performing some server management operations. When authz is enabled, any user with authentication can perform operations like shutting down the server without the ADMIN role. **CVE ID : CVE-2020-25711**		
influxdata					
kapacitor					
N/A	11-Dec-20	10	Versions of the Official kapacitor Docker images through 1.5.0-alpine contain a blank password for the root user. Systems deployed using affected versions of the kapacitor container may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-29589**	N/A	A-INF-KAPA-171220/244
infolific					
ultimate_category_excluder					
Cross-Site Request Forgery (CSRF)	11-Dec-20	6.8	The ultimate-category-excluder plugin before 1.2 for WordPress allows ultimate-category-excluder.php CSRF. **CVE ID : CVE-2020-35135**	N/A	A-INF-ULTI-171220/245
ini_project					
ini					
Uncontrolled Resource Consumption	11-Dec-20	6.8	This affects the package ini before 1.3.6. If an attacker submits a malicious INI file to an application that parses	N/A	A-INI-INI-171220/246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			it with ini.parse, they will pollute the prototype on the application. This can be exploited further depending on the context. **CVE ID : CVE-2020-7788**		
intland					
codebeamer_application_lifecycle_management					
Improper Restriction of XML External Entity Reference ('XXE')	07-Dec-20	4.3	An issue was discovered in Intland codeBeamer ALM 10.x through 10.1.SP4. The ReqIF XML data, used by the codebeamer ALM application to import projects, is parsed by insecurely configured software components, which can be abused for XML External Entity Attacks. **CVE ID : CVE-2020-26513**	N/A	A-INT-CODE-171220/247
Irssi					
docker_image					
N/A	08-Dec-20	10	The official irssi docker images before 1.1-alpine (Alpine specific) contain a blank password for a root user. System using the irssi docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-29602**	N/A	A-IRS-DOCK-171220/248
Jenkins					
installation_manager_tool					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Download of Code Without Integrity Check	03-Dec-20	10	Jenkins Plugin Installation Manager Tool 2.1.3 and earlier does not verify plugin downloads. **CVE ID : CVE-2020-2320**	https://www.jenkins.io/security/advisory/2020-12-03/#SECURITY-1856	A-JEN-INST-171220/249
shelve_project					
Cross-Site Request Forgery (CSRF)	03-Dec-20	5.8	A cross-site request forgery (CSRF) vulnerability in Jenkins Shelve Project Plugin 3.0 and earlier allows attackers to shelve, unshelve, or delete a project. **CVE ID : CVE-2020-2321**	https://www.jenkins.io/security/advisory/2020-12-03/#SECURITY-2108	A-JEN-SHEL-171220/250
cvs					
Improper Restriction of XML External Entity Reference ('XXE')	03-Dec-20	5	Jenkins CVS Plugin 2.16 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2020-2324**	https://www.jenkins.io/security/advisory/2020-12-03/#SECURITY-2146	A-JEN-CVS-171220/251
Jerryscript					
jerryscript					
Out-of-bounds Read	09-Dec-20	6.4	In JerryScript 2.3.0, there is an out-of-bounds read in main_print_unhandled_exception in the main-utils.c file. **CVE ID : CVE-2020-29657**	N/A	A-JER-JERR-171220/252
Jupyter					
oauthenticator					
Incorrect Authorization	01-Dec-20	3.5	OAuthenticator is an OAuth login mechanism for JupyterHub. In oauthenticator from version	https://github.com/jupyterhub/oauthenticato	A-JUP-OAUT-171220/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0.12.0 and before 0.12.2, the deprecated (in jupyterhub 1.2) configuration `Authenticator.whitelist`, which should be transparently mapped to `Authenticator.allowed_users` with a warning, is instead ignored by OAuthenticator classes, resulting in the same behavior as if this configuration has not been set. If this is the only mechanism of authorization restriction (i.e. no group or team restrictions in configuration) then all authenticated users will be allowed. Provider-based restrictions, including deprecated values such as `GitHubOAuthenticator.org_whitelist` are **not** affected. All users of OAuthenticator 0.12.0 and 0.12.1 with JupyterHub 1.2 (JupyterHub Helm chart 0.10.0-0.10.5) who use the `admin.whitelist.users` configuration in the jupyterhub helm chart or the `c.Authenticator.whitelist` configuration directly. Users of other deprecated configuration, e.g. `c.GitHubOAuthenticator.team_whitelist` are **not** affected. If you see a log line like this and expect a specific list of allowed usernames: "[I	r/security/advisories/GHSA-384w-5v3f-q499	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-11-27 16:51:54.528 JupyterHub app:1717] Not using allowed_users. Any authenticated user will be allowed." you are likely affected. Updating oauthenticator to 0.12.2 is recommended. A workaround is to replace the deprecated `c.Authenticator.whitelist = ...` with `c.Authenticator.allowed_users = ...`. If any users have been authorized during this time who should not have been, they must be deleted via the API or admin interface, per the referenced documentation. **CVE ID : CVE-2020-26250**		
jupyterhub					
systemdspawner					
Exposure of Resource to Wrong Sphere	09-Dec-20	3.3	jupyterhub-systemdspawner enables JupyterHub to spawn single-user notebook servers using systemd. In jupyterhub-systemdspawner before version 0.15 user API tokens issued to single-user servers are specified in the environment of systemd units. These tokens are incorrectly accessible to all users. In particular, the-littlest-jupyterhub is affected, which uses systemdspawner by default. This is patched in	https://github.com/jupyterhub/systemdspawner/security/advisories/GHSA-cg54-gpgr-4rm6	A-JUP-SYST-171220/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			jupyterhub-systemdspawner v0.15 **CVE ID : CVE-2020-26261**		
Kaspersky					
anti-ransomware_tool					
Uncontrolled Search Path Element	04-Dec-20	6.9	The installer of Kaspersky Anti-Ransomware Tool (KART) prior to KART 4.0 Patch C was vulnerable to a DLL hijacking attack that allowed an attacker to elevate privileges during installation process. **CVE ID : CVE-2020-28950**	N/A	A-KAS-ANTI-171220/255
katacontainers					
kata_containers					
N/A	07-Dec-20	9	An issue was discovered in Kata Containers through 1.11.3 and 2.x through 2.0-rc1. The runtime will execute binaries given using annotations without any kind of validation. Someone who is granted access rights to a cluster will be able to have kata-runtime execute arbitrary binaries as root on the worker nodes. **CVE ID : CVE-2020-27151**	N/A	A-KAT-KATA-171220/256
keyget_project					
keyget					
N/A	02-Dec-20	7.5	Prototype pollution vulnerability in 'keyget' versions 1.0.0 through 2.2.0 allows attacker to cause a denial of service and may	https://www.whitesourcesoftware.com/vulnerability-	A-KEY-KEYG-171220/257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to remote code execution. **CVE ID : CVE-2020-28272**	database/CVE-2020-28272	
Kubernetes					
kubernetes					
Information Exposure Through Log Files	07-Dec-20	2.1	In Kubernetes clusters using VSphere as a cloud provider, with a logging level set to 4 or above, VSphere cloud credentials will be leaked in the cloud controller manager's log. This affects < v1.19.3. **CVE ID : CVE-2020-8563**	https://github.com/kubernetes/kubernetes/issues/95621	A-KUB-KUBE-171220/258
Information Exposure Through Log Files	07-Dec-20	2.1	In Kubernetes clusters using a logging level of at least 4, processing a malformed docker config file will result in the contents of the docker config file being leaked, which can include pull secrets or other registry credentials. This affects < v1.19.3, < v1.18.10, < v1.17.13. **CVE ID : CVE-2020-8564**	https://github.com/kubernetes/kubernetes/issues/95622	A-KUB-KUBE-171220/259
Information Exposure Through Log Files	07-Dec-20	2.1	In Kubernetes, if the logging level is set to at least 9, authorization and bearer tokens will be written to log files. This can occur both in API server logs and client tool output like kubectl. This affects <= v1.19.3, <= v1.18.10, <= v1.17.13, < v1.20.0-alpha2. **CVE ID : CVE-2020-8565**	https://github.com/kubernetes/kubernetes/issues/95623	A-KUB-KUBE-171220/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure Through Log Files	07-Dec-20	2.1	In Kubernetes clusters using Ceph RBD as a storage provisioner, with logging level of at least 4, Ceph RBD admin secrets can be written to logs. This occurs in kube-controller-manager's logs during provisioning of Ceph RBD persistent claims. This affects < v1.19.3, < v1.18.10, < v1.17.13. **CVE ID : CVE-2020-8566**	https://github.com/kubernetes/kubernetes/issues/95624	A-KUB-KUBE-171220/261
lanatmservice					
m3_atm_monitoring_system					
N/A	10-Dec-20	5	In Lan ATMService M3 ATM Monitoring System 6.1.0, due to a directory-listing vulnerability, a remote attacker can view log files, located in /websocket/logs/, that contain a user's cookie values and the predefined developer's cookie value. **CVE ID : CVE-2020-29666**	N/A	A-LAN-M3_A-171220/262
Insufficient Session Expiration	10-Dec-20	10	In Lan ATMService M3 ATM Monitoring System 6.1.0, a remote attacker able to use a default cookie value, such as PHPSESSID=LANIT-IMANAGER, can achieve control over the system because of Insufficient Session Expiration. **CVE ID : CVE-2020-29667**	N/A	A-LAN-M3_A-171220/263
Lepton-cms					
leptoncms					
Improper	02-Dec-20	3.5	Lepton-CMS 4.7.0 is affected	N/A	A-LEP-LEPT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			by cross-site scripting (XSS). An attacker can inject the XSS payload in the URL field of the admin page and each time an admin visits the Menu-Pages-Pages Overview section, the XSS will be triggered. **CVE ID : CVE-2020-29240**		171220/264
Libpng					
pngcheck					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-20	4.3	A flaw was found in the check_chunk_name() function of pngcheck-2.4.0. An attacker able to pass a malicious file to be processed by pngcheck could cause a temporary denial of service, posing a low risk to application availability. **CVE ID : CVE-2020-27818**	https://bugzilla.redhat.com/show_bug.cgi?id=1902011	A-LIB-PNGC-171220/265
lightbend					
play_framework					
N/A	03-Dec-20	4	An issue was discovered in Play Framework 2.8.0 through 2.8.4. Carefully crafted JSON payloads sent as a form field lead to Data Amplification. This affects users migrating from a Play version prior to 2.8.0 that used the Play Java API to serialize classes with protected or private fields to JSON. **CVE ID : CVE-2020-28923**	https://www.playframework.com/security/vulnerability/CVE-2020-28923-ImproperRemovalofSensitiveInformationBeforeStorageorTransfer	A-LIG-PLAY-171220/266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Linuxfoundation					
containerd					
Incorrect Resource Transfer Between Spheres	01-Dec-20	3.6	containerd is an industry-standard container runtime and is available as a daemon for Linux and Windows. In containerd before versions 1.3.9 and 1.4.3, the containerd-shim API is improperly exposed to host network containers. Access controls for the shim's API socket verified that the connecting process had an effective UID of 0, but did not otherwise restrict access to the abstract Unix domain socket. This would allow malicious containers running in the same network namespace as the shim, with an effective UID of 0 but otherwise reduced privileges, to cause new processes to be run with elevated privileges. This vulnerability has been fixed in containerd 1.3.9 and 1.4.3. Users should update to these versions as soon as they are released. It should be noted that containers started with an old version of containerd-shim should be stopped and restarted, as running containers will continue to be vulnerable even after an upgrade. If you are not providing the ability for untrusted users to start	https://github.com/containerd/containerd/security/advisories/GHSA-36xw-fx78-c5r4	A-LIN-CONT-171220/267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			containers in the same network namespace as the shim (typically the "host" network namespace, for example with docker run --net=host or hostNetwork: true in a Kubernetes pod) and run with an effective UID of 0, you are not vulnerable to this issue. If you are running containers with a vulnerable configuration, you can deny access to all abstract sockets with AppArmor by adding a line similar to deny unix addr=@**, to your policy. It is best practice to run containers with a reduced set of privileges, with a non-zero UID, and with isolated namespaces. The containerd maintainers strongly advise against sharing namespaces with the host. Reducing the set of isolation mechanisms used for a container necessarily increases that container's privilege, regardless of what container runtime is used for running that container. **CVE ID : CVE-2020-15257**		
spinnaker					
Deserialization of Untrusted Data	11-Dec-20	6.5	Nolan Ray from Apple Information Security identified a security vulnerability in Spinnaker, all versions prior to version	https://github.com/Netflix/security-bulletins/bl	A-LIN-SPIN-171220/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.23.4, 1.22.4 or 1.21.5. The vulnerability exists within the handling of SpEL expressions that allows an attacker to read and write arbitrary files within the orca container via authenticated HTTP POST requests. **CVE ID : CVE-2020-9301**	ob/master/advisories/nflx-2020-006.md	
logicaldoc					
logicaldoc					
Incorrect Default Permissions	03-Dec-20	7.2	A local privilege elevation vulnerability exists in the file system permissions of LogicalDoc 8.5.1 installation. Depending on the vector chosen, an attacker can either replace the service binary or replace DLL files loaded by the service, both which get executed by a service thus executing arbitrary commands with System privileges. **CVE ID : CVE-2020-13542**	N/A	A-LOG-LOGI-171220/269
Lxml					
lxml					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Dec-20	4.3	A XSS vulnerability was discovered in python-lxml's clean module. The module's parser didn't properly imitate browsers, which caused different behaviors between the sanitizer and the user's page. A remote attacker could exploit this flaw to run arbitrary	N/A	A-LXM-LXML-171220/270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML/JS code. **CVE ID : CVE-2020-27783**		
macrium					
reflect					
Improper Privilege Management	09-Dec-20	7.2	Macrium Reflect includes an OpenSSL component that specifies an OPENSSLDIR variable as C:\openssl\. Macrium Reflect contains a privileged service that uses this OpenSSL component. Because unprivileged Windows users can create subdirectories off of the system root, a user can create the appropriate path to a specially-crafted openssl.cnf file to achieve arbitrary code execution with SYSTEM privileges. **CVE ID : CVE-2020-10143**	N/A	A-MAC-REFL-171220/271
matomo					
docker					
N/A	08-Dec-20	10	The official piwik Docker images before fpm-alpine (Alpine specific) contain a blank password for a root user. Systems using the Piwik Docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access. **CVE ID : CVE-2020-29578**	N/A	A-MAT-DOCK-171220/272
Matrix					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
synapse					
Uncontrolled Resource Consumption	09-Dec-20	4	Matrix is an ecosystem for open federated Instant Messaging and VoIP. Synapse is a reference "homeserver" implementation of Matrix. A malicious or poorly-implemented homeserver can inject malformed events into a room by specifying a different room id in the path of a `/send_join`, `/send_leave`, `/invite` or `/exchange_third_party_invite` request. This can lead to a denial of service in which future events will not be correctly sent to other servers over federation. This affects any server which accepts federation requests from untrusted servers. The Matrix Synapse reference implementation before version 1.23.1 the implementation is vulnerable to this injection attack. Issue is fixed in version 1.23.1. As a workaround homeserver administrators could limit access to the federation API to trusted servers (for example via `federation_domain_whitelist`). **CVE ID : CVE-2020-26257**	https://github.com/matrix-org/synapse/security/advisories/GHSA-hxmp-pqch-c8mm	A-MAT-SYNA-171220/273
Mcafee					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
virusscan_enterprise					
Incorrect Permission Assignment for Critical Resource	09-Dec-20	4.6	Incorrect Permission Assignment for Critical Resource vulnerability in McAfee VirusScan Enterprise (VSE) prior to 8.8 Patch 16 allows local administrators to bypass local security protection through VSE not correctly integrating with Windows Defender Application Control via careful manipulation of the Code Integrity checks. **CVE ID : CVE-2020-7337**	https://kc.mcafee.com/corporate/index?page=content&id=SB10338	A-MCA-VIRU-171220/274
total_protection					
Improper Privilege Management	01-Dec-20	4.4	Privilege Escalation vulnerability in Microsoft Windows client McAfee Total Protection (MTP) prior to 16.0.29 allows local users to gain elevated privileges via careful manipulation of a folder by creating a junction link. This exploits a lack of protection through a timing issue and is only exploitable in a small time window. **CVE ID : CVE-2020-7335**	http://service.mcafee.com/FAQDocument.aspx?&id=TS103089	A-MCA-TOTA-171220/275
database_security					
Use of a Broken or Risky Cryptographic Algorithm	10-Dec-20	5.8	Use of a Broken or Risky Cryptographic Algorithm vulnerability in McAfee Database Security Server and Sensor prior to 4.8.0 in the form of a SHA1 signed certificate that would allow an attacker on the same local	N/A	A-MCA-DATA-171220/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network to potentially intercept communication between the Server and Sensors. **CVE ID : CVE-2020-7339**		
Microchip					
mplab_harmony					
Out-of-bounds Read	11-Dec-20	6.4	An issue was discovered in picoTCP 1.7.0. The code for processing the IPv6 headers does not validate whether the IPv6 payload length field is equal to the actual size of the payload, which leads to an Out-of-Bounds read during the ICMPv6 checksum calculation, resulting in either Denial-of-Service or Information Disclosure. This affects pico_ipv6_extension_headers and pico_checksum_adder (in pico_ipv6.c and pico_frame.c). **CVE ID : CVE-2020-17441**	N/A	A-MIC-MPLA-171220/277
Microfocus					
filr					
Information Exposure	11-Dec-20	4	Unauthorized disclosure of sensitive information vulnerability in Micro Focus Filr product. Affecting all 3.x and 4.x versions. The vulnerability could be exploited to disclose unauthorized sensitive information. **CVE ID : CVE-2020-25838**	https://softwaresupport.softwaregrp.com/doc/KM03767186	A-MIC-FILR-171220/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Microsoft					
365_apps					
N/A	10-Dec-20	5	, aka 'Microsoft Outlook Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17119**	N/A	A-MIC-365_-171220/279
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17125, CVE-2020-17127, CVE-2020-17128, CVE-2020-17129. **CVE ID : CVE-2020-17123**	N/A	A-MIC-365_-171220/280
N/A	10-Dec-20	9.3	, aka 'Microsoft PowerPoint Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17124**	N/A	A-MIC-365_-171220/281
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17127, CVE-2020-17128, CVE-2020-17129. **CVE ID : CVE-2020-17125**	N/A	A-MIC-365_-171220/282
N/A	10-Dec-20	2.1	, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17126**	N/A	A-MIC-365_-171220/283
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17125, CVE-2020-	N/A	A-MIC-365_-171220/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17127, CVE-2020-17129. **CVE ID : CVE-2020-17128**		
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17125, CVE-2020-17127, CVE-2020-17128. **CVE ID : CVE-2020-17129**	N/A	A-MIC-365_-171220/285
N/A	10-Dec-20	6	, aka 'Microsoft Excel Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-17130**	N/A	A-MIC-365_-171220/286
office_web_apps					
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17123, CVE-2020-17125, CVE-2020-17127, CVE-2020-17128, CVE-2020-17129. **CVE ID : CVE-2020-17122**	N/A	A-MIC-OFFI-171220/287
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17125, CVE-2020-17127, CVE-2020-17128, CVE-2020-17129. **CVE ID : CVE-2020-17123**	N/A	A-MIC-OFFI-171220/288
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17127, CVE-2020-	N/A	A-MIC-OFFI-171220/289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17128, CVE-2020-17129. **CVE ID : CVE-2020-17125**		
N/A	10-Dec-20	2.1	, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17126**	N/A	A-MIC-OFFI-171220/290
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17125, CVE-2020-17127, CVE-2020-17129. **CVE ID : CVE-2020-17128**	N/A	A-MIC-OFFI-171220/291
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17125, CVE-2020-17127, CVE-2020-17128. **CVE ID : CVE-2020-17129**	N/A	A-MIC-OFFI-171220/292
powerpoint					
N/A	10-Dec-20	9.3	, aka 'Microsoft PowerPoint Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17124**	N/A	A-MIC-POWE-171220/293
azure_sdk_for_java					
N/A	10-Dec-20	6.4	, aka 'Azure SDK for Java Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16971**	N/A	A-MIC-AZUR-171220/294
git_credential_manager_core					
Use of Incorrectly-	08-Dec-20	3.6	Git Credential Manager Core (GCM Core) is a secure Git	https://github.com/mic	A-MIC-GIT_-171220/295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resolved Name or Reference			credential helper built on .NET Core that runs on Windows and macOS. In Git Credential Manager Core before version 2.0.289, when recursively cloning a Git repository on Windows with submodules, Git will first clone the top-level repository and then recursively clone all submodules by starting new Git processes from the top-level working directory. If a malicious git.exe executable is present in the top-level repository then this binary will be started by Git Credential Manager Core when attempting to read configuration, and not git.exe as found on the %PATH%. This only affects GCM Core on Windows, not macOS or Linux-based distributions. GCM Core version 2.0.289 contains the fix for this vulnerability, and is available from the project's GitHub releases page. GCM Core 2.0.289 is also bundled in the latest Git for Windows release; version 2.29.2(3). As a workaround, users should avoid recursively cloning untrusted repositories with the --recurse-submodules option. **CVE ID : CVE-2020-26233**	rosoft/Git-Credential-Manager-Core/security/advisories/GHSA-2gq7-ww4j-3m76	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c_sdk_for_azure_iot					
N/A	10-Dec-20	9.4	, aka 'Azure SDK for C Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-17002**	N/A	A-MIC-C_SD-171220/296
outlook_2013_rt					
N/A	10-Dec-20	5	, aka 'Microsoft Outlook Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17119**	N/A	A-MIC-OUTL-171220/297
chakracore					
Out-of-bounds Write	10-Dec-20	5.1	, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-17131**	N/A	A-MIC-CHAK-171220/298
edge					
Out-of-bounds Write	10-Dec-20	5.1	, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-17131**	N/A	A-MIC-EDGE-171220/299
Improper Input Validation	10-Dec-20	5.8	, aka 'Microsoft Edge for Android Spoofing Vulnerability'. **CVE ID : CVE-2020-17153**	N/A	A-MIC-EDGE-171220/300
office					
N/A	10-Dec-20	5	, aka 'Microsoft Outlook Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17119**	N/A	A-MIC-OFFI-171220/301
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17123, CVE-2020-17125, CVE-2020-17127, CVE-2020-	N/A	A-MIC-OFFI-171220/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17128, CVE-2020-17129. **CVE ID : CVE-2020-17122**		
N/A	10-Dec-20	9.3	, aka 'Microsoft PowerPoint Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17124**	N/A	A-MIC-OFFI-171220/303
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17127, CVE-2020-17128, CVE-2020-17129. **CVE ID : CVE-2020-17125**	N/A	A-MIC-OFFI-171220/304
N/A	10-Dec-20	2.1	, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17126**	N/A	A-MIC-OFFI-171220/305
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17125, CVE-2020-17127, CVE-2020-17129. **CVE ID : CVE-2020-17128**	N/A	A-MIC-OFFI-171220/306
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17125, CVE-2020-17127, CVE-2020-17128. **CVE ID : CVE-2020-17129**	N/A	A-MIC-OFFI-171220/307
visual_studio_2017					
Improper	10-Dec-20	6.8	, aka 'Visual Studio Remote	N/A	A-MIC-VISU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control of Generation of Code ('Code Injection')			Code Execution Vulnerability'. **CVE ID : CVE-2020-17156**		171220/308
sharepoint_server					
Improper Input Validation	10-Dec-20	6	, aka 'Microsoft SharePoint Spoofing Vulnerability'. **CVE ID : CVE-2020-17115**	N/A	A-MIC-SHAR-171220/309
N/A	10-Dec-20	10	, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17121. **CVE ID : CVE-2020-17118**	N/A	A-MIC-SHAR-171220/310
N/A	10-Dec-20	4	, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17120**	N/A	A-MIC-SHAR-171220/311
N/A	10-Dec-20	6.5	, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17118. **CVE ID : CVE-2020-17121**	N/A	A-MIC-SHAR-171220/312
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17123, CVE-2020-17125, CVE-2020-17127, CVE-2020-17128, CVE-2020-17129. **CVE ID : CVE-2020-17122**	N/A	A-MIC-SHAR-171220/313
Improper Privilege Management	10-Dec-20	6	, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'.	N/A	A-MIC-SHAR-171220/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-17089		
outlook					
N/A	10-Dec-20	5	, aka 'Microsoft Outlook Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17119**	N/A	A-MIC-OUTL-171220/315
office_online_server					
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17125, CVE-2020-17127, CVE-2020-17128, CVE-2020-17129. **CVE ID : CVE-2020-17123**	N/A	A-MIC-OFFI-171220/316
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17127, CVE-2020-17128, CVE-2020-17129. **CVE ID : CVE-2020-17125**	N/A	A-MIC-OFFI-171220/317
N/A	10-Dec-20	2.1	, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17126**	N/A	A-MIC-OFFI-171220/318
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17125, CVE-2020-17127, CVE-2020-17129. **CVE ID : CVE-2020-17128**	N/A	A-MIC-OFFI-171220/319
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel	N/A	A-MIC-OFFI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17125, CVE-2020-17127, CVE-2020-17128. **CVE ID : CVE-2020-17129**		171220/320
exchange_server					
N/A	10-Dec-20	9	, aka 'Microsoft Exchange Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17132, CVE-2020-17141, CVE-2020-17142, CVE-2020-17144. **CVE ID : CVE-2020-17117**	N/A	A-MIC-EXCH-171220/321
Improper Control of Generation of Code ('Code Injection')	10-Dec-20	6.5	, aka 'Microsoft Exchange Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17117, CVE-2020-17141, CVE-2020-17142, CVE-2020-17144. **CVE ID : CVE-2020-17132**	N/A	A-MIC-EXCH-171220/322
Improper Control of Generation of Code ('Code Injection')	10-Dec-20	6	, aka 'Microsoft Exchange Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17117, CVE-2020-17132, CVE-2020-17142, CVE-2020-17144. **CVE ID : CVE-2020-17141**	N/A	A-MIC-EXCH-171220/323
Improper Control of Generation of Code ('Code	10-Dec-20	6.5	, aka 'Microsoft Exchange Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17117, CVE-2020-17132,	N/A	A-MIC-EXCH-171220/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			CVE-2020-17141, CVE-2020-17144. **CVE ID : CVE-2020-17142**		
Information Exposure	10-Dec-20	6.5	, aka 'Microsoft Exchange Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17143**	N/A	A-MIC-EXCH-171220/325
Improper Control of Generation of Code ('Code Injection')	10-Dec-20	6	, aka 'Microsoft Exchange Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17117, CVE-2020-17132, CVE-2020-17141, CVE-2020-17142. **CVE ID : CVE-2020-17144**	N/A	A-MIC-EXCH-171220/326
sharepoint_foundation					
Improper Input Validation	10-Dec-20	6	, aka 'Microsoft SharePoint Spoofing Vulnerability'. **CVE ID : CVE-2020-17115**	N/A	A-MIC-SHAR-171220/327
N/A	10-Dec-20	10	, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17121. **CVE ID : CVE-2020-17118**	N/A	A-MIC-SHAR-171220/328
N/A	10-Dec-20	4	, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17120**	N/A	A-MIC-SHAR-171220/329
N/A	10-Dec-20	6.5	, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17118. **CVE ID : CVE-2020-17121**	N/A	A-MIC-SHAR-171220/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	10-Dec-20	6	, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17089**	N/A	A-MIC-SHAR-171220/331
team_foundation_server					
Improper Input Validation	10-Dec-20	4.9	, aka 'Azure DevOps Server and Team Foundation Services Spoofing Vulnerability'. **CVE ID : CVE-2020-17145**	N/A	A-MIC-TEAM-171220/332
excel					
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17125, CVE-2020-17127, CVE-2020-17128, CVE-2020-17129. **CVE ID : CVE-2020-17123**	N/A	A-MIC-EXCE-171220/333
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17127, CVE-2020-17128, CVE-2020-17129. **CVE ID : CVE-2020-17125**	N/A	A-MIC-EXCE-171220/334
N/A	10-Dec-20	2.1	, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17126**	N/A	A-MIC-EXCE-171220/335
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123,	N/A	A-MIC-EXCE-171220/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-17125, CVE-2020-17128, CVE-2020-17129. **CVE ID : CVE-2020-17127**		
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17125, CVE-2020-17127, CVE-2020-17129. **CVE ID : CVE-2020-17128**	N/A	A-MIC-EXCE-171220/337
N/A	10-Dec-20	9.3	, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17122, CVE-2020-17123, CVE-2020-17125, CVE-2020-17127, CVE-2020-17128. **CVE ID : CVE-2020-17129**	N/A	A-MIC-EXCE-171220/338
N/A	10-Dec-20	6	, aka 'Microsoft Excel Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-17130**	N/A	A-MIC-EXCE-171220/339
visual_studio_code					
Improper Control of Generation of Code ('Code Injection')	10-Dec-20	6.8	, aka 'Visual Studio Code Remote Development Extension Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17148**	N/A	A-MIC-VISU-171220/340
Improper Control of Generation of Code ('Code Injection')	10-Dec-20	6.8	, aka 'Visual Studio Code Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17150**	N/A	A-MIC-VISU-171220/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	10-Dec-20	6.8	, aka 'Visual Studio Code Java Extension Pack Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17159**	N/A	A-MIC-VISU-171220/342
visual_studio_2019					
Improper Control of Generation of Code ('Code Injection')	10-Dec-20	6.8	, aka 'Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17156**	N/A	A-MIC-VISU-171220/343
dynamics_365					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	3.5	, aka 'Dynamics CRM Webclient Cross-site Scripting Vulnerability'. **CVE ID : CVE-2020-17147**	N/A	A-MIC-DYNA-171220/344
Improper Control of Generation of Code ('Code Injection')	10-Dec-20	6.5	, aka 'Microsoft Dynamics 365 for Finance and Operations (on-premises) Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17158. **CVE ID : CVE-2020-17152**	N/A	A-MIC-DYNA-171220/345
Improper Control of Generation of Code ('Code Injection')	10-Dec-20	6.5	, aka 'Microsoft Dynamics 365 for Finance and Operations (on-premises) Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17152.	N/A	A-MIC-DYNA-171220/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-17158		
teams					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	3.5	The Microsoft Teams online service contains a stored cross-site scripting vulnerability in the displayName parameter that can be exploited on Teams clients to obtain sensitive information such as authentication tokens and to possibly execute arbitrary commands. This vulnerability was fixed for all Teams users in the online service on or around October 2020. **CVE ID : CVE-2020-10146**	N/A	A-MIC-TEAM-171220/347
dynamics_nav					
Information Exposure	10-Dec-20	4	, aka 'Microsoft Dynamics Business Central/NAV Information Disclosure'. **CVE ID : CVE-2020-17133**	N/A	A-MIC-DYNA-171220/348
Misp					
misp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-20	4.3	app/View/Elements/genericElements/SingleViews/Fields/genericField.ctp in MISP 2.4.135 has XSS via the authkey comment field. **CVE ID : CVE-2020-29572**	N/A	A-MIS-MISP-171220/349
moddable					
moddable					
N/A	04-Dec-20	5	Invalid Memory Access in	N/A	A-MOD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the fxProxyGetter function in moddable/xs/sources/xsProxy.c in Moddable SDK before OS200908 causes a denial of service (SEGV). **CVE ID : CVE-2020-25461**		MODD-171220/350
Out-of-bounds Write	04-Dec-20	7.5	Heap buffer overflow in the fxCheckArrowFunction function at moddable/xs/sources/xsSyntaxical.c:3562 in Moddable SDK before OS200903. **CVE ID : CVE-2020-25462**	N/A	A-MOD-MODD-171220/351
N/A	04-Dec-20	5	Invalid Memory Access in fxUTF8Decode at moddable/xs/sources/xsCommon.c:916 in Moddable SDK before OS200908 causes a denial of service (SEGV). **CVE ID : CVE-2020-25463**	N/A	A-MOD-MODD-171220/352
Out-of-bounds Write	04-Dec-20	5	Heap buffer overflow at moddable/xs/sources/xsDebug.c in Moddable SDK before before 20200903. The top stack frame is only partially initialized because the stack overflowed while creating the frame. This leads to a crash in the code sending the stack frame to the debugger. **CVE ID : CVE-2020-25464**	N/A	A-MOD-MODD-171220/353
NULL Pointer Dereference	04-Dec-20	5	Null Pointer Dereference. in xObjectBindingFromExpression at moddable/xs/sources/xsSyntaxical.c:3419 in Moddable	N/A	A-MOD-MODD-171220/354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDK before OS200908 causes a denial of service (SEGV). **CVE ID : CVE-2020-25465**		
Moodle					
moodle					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	4.3	The moodlenetprofile user profile field required extra sanitizing to prevent a stored XSS risk. This affects versions 3.9 to 3.9.1. Fixed in 3.9.2. **CVE ID : CVE-2020-25627**	https://moodle.org/mod/forum/discuss.php?d=410839	A-MOO-MOOD-171220/355
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-20	4.3	The filter in the tag manager required extra sanitizing to prevent a reflected XSS risk. This affects 3.9 to 3.9.1, 3.8 to 3.8.4, 3.7 to 3.7.7, 3.5 to 3.5.13 and earlier unsupported versions. Fixed in 3.9.2, 3.8.5, 3.7.8 and 3.5.14. **CVE ID : CVE-2020-25628**	https://moodle.org/mod/forum/discuss.php?d=410840	A-MOO-MOOD-171220/356
Improper Access Control	08-Dec-20	6.5	A vulnerability was found in Moodle where users with "Log in as" capability in a course context (typically, course managers) may gain access to some site administration capabilities by "logging in as" a System manager. This affects 3.9 to 3.9.1, 3.8 to 3.8.4, 3.7 to 3.7.7, 3.5 to 3.5.13 and earlier unsupported versions. This is fixed in 3.9.2, 3.8.5, 3.7.8 and 3.5.14.	https://moodle.org/mod/forum/discuss.php?d=410841	A-MOO-MOOD-171220/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-25629		
Uncontrolled Resource Consumption	08-Dec-20	5	A vulnerability was found in Moodle where the decompressed size of zip files was not checked against available user quota before unzipping them, which could lead to a denial of service risk. This affects versions 3.9 to 3.9.1, 3.8 to 3.8.4, 3.7 to 3.7.7, 3.5 to 3.5.13 and earlier unsupported versions. Fixed in 3.9.2, 3.8.5, 3.7.8 and 3.5.14. **CVE ID : CVE-2020-25630**	https://moodle.org/mod/forum/discuss.php?d=410842	A-MOO-MOOD-171220/358
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-20	4.3	A vulnerability was found in Moodle 3.9 to 3.9.1, 3.8 to 3.8.4 and 3.7 to 3.7.7 where it was possible to include JavaScript in a book's chapter title, which was not escaped on the "Add new chapter" page. This is fixed in 3.9.2, 3.8.5 and 3.7.8. **CVE ID : CVE-2020-25631**	https://moodle.org/mod/forum/discuss.php?d=410843	A-MOO-MOOD-171220/359
moutjs					
mout					
N/A	11-Dec-20	7.5	This affects all versions of package mout. The deepFillIn function can be used to 'fill missing properties recursively', while the deepMixIn 'mixes objects into the target object, recursively mixing existing child objects as well'. In both cases, the key used to access the target object recursively	https://github.com/mout/mout/blob/master/src/object/deepFillIn.js, https://github.com/mout/mout/blob/master/	A-MOU-MOUT-171220/360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is not checked, leading to a Prototype Pollution. **CVE ID : CVE-2020-7792**	src/object/deepMixIn.js, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1050374, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1050373	
Mozilla					
firefox					
Use After Free	09-Dec-20	9.3	In certain circumstances, the MCallGetProperty opcode can be emitted with unmet assumptions resulting in an exploitable use-after-free condition. This vulnerability affects Firefox < 82.0.3, Firefox ESR < 78.4.1, and Thunderbird < 78.4.2. **CVE ID : CVE-2020-26950**	https://www.mozilla.org/security/advisories/mfsa2020-49/	A-MOZ-FIRE-171220/361
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	4.3	A parsing and event loading mismatch in Firefox's SVG code could have allowed load events to fire, even after sanitization. An attacker already capable of exploiting an XSS vulnerability in privileged internal pages could have used this attack to bypass our built-in sanitizer. This vulnerability affects Firefox < 83, Firefox	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/,	A-MOZ-FIRE-171220/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26951**	https://www.mozilla.org/security/advisories/mfsa2020-52/	
Out-of-bounds Write	09-Dec-20	9.3	Incorrect bookkeeping of functions inlined during JIT compilation could have led to memory corruption and a potentially exploitable crash when handling out-of-memory errors. This vulnerability affects Firefox < 83. **CVE ID : CVE-2020-26952**	https://www.mozilla.org/security/advisories/mfsa2020-50/	A-MOZ-FIRE-171220/363
Improper Restriction of Rendered UI Layers or Frames	09-Dec-20	4.3	It was possible to cause the browser to enter fullscreen mode without displaying the security UI; thus making it possible to attempt a phishing attack or otherwise confuse the user. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26953**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-FIRE-171220/364
N/A	09-Dec-20	4.3	When accepting a malicious intent from other installed apps, Firefox for Android accepted manifests from arbitrary file paths and	https://www.mozilla.org/security/advisories/mfsa2020-	A-MOZ-FIRE-171220/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowed declaring webapp manifests for other origins. This could be used to gain fullscreen access for UI spoofing and could also lead to cross-origin attacks on targeted websites. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83. **CVE ID : CVE-2020-26954**	50/	
Reliance on Cookies without Validation and Integrity Checking	09-Dec-20	4.3	When a user downloaded a file in Firefox for Android, if a cookie is set, it would have been re-sent during a subsequent file download operation on the same domain, regardless of whether the original and subsequent request were in private and non-private browsing modes. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83. **CVE ID : CVE-2020-26955**	https://www.mozilla.org/security/advisories/mfsa2020-50/	A-MOZ-FIRE-171220/366
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	4.3	In some cases, removing HTML elements during sanitization would keep existing SVG event handlers and therefore lead to XSS. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird <	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.o	A-MOZ-FIRE-171220/367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			78.5. **CVE ID : CVE-2020-26956**	rg/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	
Improper Initialization	09-Dec-20	4.3	OneCRL was non-functional in the new Firefox for Android due to a missing service initialization. This could result in a failure to enforce some certificate revocations. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83. **CVE ID : CVE-2020-26957**	https://www.mozilla.org/security/advisories/mfsa2020-50/	A-MOZ-FIRE-171220/368
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	4.3	Firefox did not block execution of scripts with incorrect MIME types when the response was intercepted and cached through a ServiceWorker. This could lead to a cross-site script inclusion vulnerability, or a Content Security Policy bypass. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26958**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories	A-MOZ-FIRE-171220/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/mfsa2020-52/	
Use After Free	09-Dec-20	6.8	During browser shutdown, reference decrementing could have occured on a previously freed object, resulting in a use-after-free, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26959**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-FIRE-171220/370
Use After Free	09-Dec-20	9.3	If the Compact() method was called on an nsTArray, the array could have been reallocated without updating other pointers, leading to a potential use-after-free and exploitable crash. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26960**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-FIRE-171220/371
N/A	09-Dec-20	4.3	When DNS over HTTPS is in	https://ww	A-MOZ-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use, it intentionally filters RFC1918 and related IP ranges from the responses as these do not make sense coming from a DoH resolver. However when an IPv4 address was mapped through IPv6, these addresses were erroneously let through, leading to a potential DNS Rebinding attack. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26961**	w.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	171220/372
Improper Restriction of Rendered UI Layers or Frames	09-Dec-20	4.3	Cross-origin iframes that contained a login form could have been recognized by the login autofill service, and populated. This could have been used in clickjacking attacks, as well as be read across partitions in dynamic first party isolation. This vulnerability affects Firefox < 83. **CVE ID : CVE-2020-26962**	https://www.mozilla.org/security/advisories/mfsa2020-50/	A-MOZ-FIRE-171220/373
N/A	09-Dec-20	4.3	Repeated calls to the history and location interfaces could have been used to hang the browser. This was addressed by introducing rate-limiting to these API calls. This vulnerability affects Firefox < 83. **CVE ID : CVE-2020-26963**	https://www.mozilla.org/security/advisories/mfsa2020-50/	A-MOZ-FIRE-171220/374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Dec-20	4	If the Remote Debugging via USB feature was enabled in Firefox for Android on an Android version prior to Android 6.0, untrusted apps could have connected to the feature and operated with the privileges of the browser to read and interact with web content. The feature was implemented as a unix domain socket, protected by the Android SELinux policy; however, SELinux was not enforced for versions prior to 6.0. This was fixed by removing the Remote Debugging via USB feature from affected devices. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83. **CVE ID : CVE-2020-26964**	https://www.mozilla.org/security/advisories/mfsa2020-50/	A-MOZ-FIRE-171220/375
Improper Cross-boundary Removal of Sensitive Data	09-Dec-20	4.3	Some websites have a feature "Show Password" where clicking a button will change a password field into a textbook field, revealing the typed password. If, when using a software keyboard that remembers user input, a user typed their password and used that feature, the type of the password field was changed, resulting in a keyboard layout change and the possibility for the	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.o	A-MOZ-FIRE-171220/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			software keyboard to remember the typed password. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26965**	rg/security /advisories /mfsa2020-52/	
N/A	09-Dec-20	4.3	Searching for a single word from the address bar caused an mDNS request to be sent on the local network searching for a hostname consisting of that string; resulting in an information leak. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26966**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-FIRE-171220/377
N/A	09-Dec-20	4.3	When listening for page changes with a Mutation Observer, a malicious web page could confuse Firefox Screenshots into interacting with elements other than those that it injected into the page. This would lead to internal errors and unexpected behavior in the Screenshots code. This vulnerability affects Firefox < 83. **CVE ID : CVE-2020-26967**	https://www.mozilla.org/security/advisories/mfsa2020-50/	A-MOZ-FIRE-171220/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	09-Dec-20	9.3	Mozilla developers reported memory safety bugs present in Firefox 82 and Firefox ESR 78.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26968**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-FIRE-171220/379
Out-of-bounds Write	09-Dec-20	9.3	Mozilla developers reported memory safety bugs present in Firefox 82. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 83. **CVE ID : CVE-2020-26969**	https://www.mozilla.org/security/advisories/mfsa2020-50/	A-MOZ-FIRE-171220/380
firefox_esr					
Use After Free	09-Dec-20	9.3	In certain circumstances, the MCallGetProperty opcode can be emitted with unmet assumptions resulting in an exploitable use-after-free condition. This vulnerability affects Firefox < 82.0.3, Firefox ESR < 78.4.1, and	https://www.mozilla.org/security/advisories/mfsa2020-49/	A-MOZ-FIRE-171220/381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 78.4.2. **CVE ID : CVE-2020-26950**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	4.3	A parsing and event loading mismatch in Firefox's SVG code could have allowed load events to fire, even after sanitization. An attacker already capable of exploiting an XSS vulnerability in privileged internal pages could have used this attack to bypass our built-in sanitizer. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26951**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-FIRE-171220/382
Improper Restriction of Rendered UI Layers or Frames	09-Dec-20	4.3	It was possible to cause the browser to enter fullscreen mode without displaying the security UI; thus making it possible to attempt a phishing attack or otherwise confuse the user. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26953**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-FIRE-171220/383
Improper	09-Dec-20	4.3	In some cases, removing	https://ww	A-MOZ-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			HTML elements during sanitization would keep existing SVG event handlers and therefore lead to XSS. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26956**	w.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	171220/384
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	4.3	Firefox did not block execution of scripts with incorrect MIME types when the response was intercepted and cached through a ServiceWorker. This could lead to a cross-site script inclusion vulnerability, or a Content Security Policy bypass. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26958**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-FIRE-171220/385
Use After Free	09-Dec-20	6.8	During browser shutdown, reference decrementing could have occured on a previously freed object, resulting in a use-after-free,	https://www.mozilla.org/security/advisories/mfsa2020-	A-MOZ-FIRE-171220/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26959**	50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	
Use After Free	09-Dec-20	9.3	If the Compact() method was called on an nsTArray, the array could have been reallocated without updating other pointers, leading to a potential use-after-free and exploitable crash. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26960**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-FIRE-171220/387
N/A	09-Dec-20	4.3	When DNS over HTTPS is in use, it intentionally filters RFC1918 and related IP ranges from the responses as these do not make sense coming from a DoH resolver. However when an IPv4 address was mapped through IPv6, these	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security	A-MOZ-FIRE-171220/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			addresses were erroneously let through, leading to a potential DNS Rebinding attack. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26961**	/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	
Improper Cross-boundary Removal of Sensitive Data	09-Dec-20	4.3	Some websites have a feature "Show Password" where clicking a button will change a password field into a textbook field, revealing the typed password. If, when using a software keyboard that remembers user input, a user typed their password and used that feature, the type of the password field was changed, resulting in a keyboard layout change and the possibility for the software keyboard to remember the typed password. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26965**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-FIRE-171220/389
N/A	09-Dec-20	4.3	Searching for a single word from the address bar caused an mDNS request to be sent on the local network searching for a hostname consisting of that string; resulting in an information leak. *Note: This issue only affected Windows operating	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security	A-MOZ-FIRE-171220/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26966**	/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	
Out-of-bounds Write	09-Dec-20	9.3	Mozilla developers reported memory safety bugs present in Firefox 82 and Firefox ESR 78.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26968**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-FIRE-171220/391
thunderbird					
Use After Free	09-Dec-20	9.3	In certain circumstances, the MCallGetProperty opcode can be emitted with unmet assumptions resulting in an exploitable use-after-free condition. This vulnerability affects Firefox < 82.0.3, Firefox ESR < 78.4.1, and Thunderbird < 78.4.2. **CVE ID : CVE-2020-26950**	https://www.mozilla.org/security/advisories/mfsa2020-49/	A-MOZ-THUN-171220/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	4.3	A parsing and event loading mismatch in Firefox's SVG code could have allowed load events to fire, even after sanitization. An attacker already capable of exploiting an XSS vulnerability in privileged internal pages could have used this attack to bypass our built-in sanitizer. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26951**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-THUN-171220/393
Improper Restriction of Rendered UI Layers or Frames	09-Dec-20	4.3	It was possible to cause the browser to enter fullscreen mode without displaying the security UI; thus making it possible to attempt a phishing attack or otherwise confuse the user. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26953**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-THUN-171220/394
Improper Neutralization of Input During Web	09-Dec-20	4.3	In some cases, removing HTML elements during sanitization would keep existing SVG event handlers	https://www.mozilla.org/security/advisories	A-MOZ-THUN-171220/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			and therefore lead to XSS. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26956**	/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	4.3	Firefox did not block execution of scripts with incorrect MIME types when the response was intercepted and cached through a ServiceWorker. This could lead to a cross-site script inclusion vulnerability, or a Content Security Policy bypass. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26958**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-THUN-171220/396
Use After Free	09-Dec-20	6.8	During browser shutdown, reference decrementing could have occured on a previously freed object, resulting in a use-after-free, memory corruption, and a potentially exploitable crash. This vulnerability affects	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.o	A-MOZ-THUN-171220/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26959**	rg/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	
Use After Free	09-Dec-20	9.3	If the Compact() method was called on an nsTArray, the array could have been reallocated without updating other pointers, leading to a potential use-after-free and exploitable crash. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26960**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-THUN-171220/398
N/A	09-Dec-20	4.3	When DNS over HTTPS is in use, it intentionally filters RFC1918 and related IP ranges from the responses as these do not make sense coming from a DoH resolver. However when an IPv4 address was mapped through IPv6, these addresses were erroneously let through, leading to a potential DNS Rebinding	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/,	A-MOZ-THUN-171220/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26961**	https://www.mozilla.org/security/advisories/mfsa2020-52/	
Improper Cross-boundary Removal of Sensitive Data	09-Dec-20	4.3	Some websites have a feature "Show Password" where clicking a button will change a password field into a textbook field, revealing the typed password. If, when using a software keyboard that remembers user input, a user typed their password and used that feature, the type of the password field was changed, resulting in a keyboard layout change and the possibility for the software keyboard to remember the typed password. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26965**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-THUN-171220/400
N/A	09-Dec-20	4.3	Searching for a single word from the address bar caused an mDNS request to be sent on the local network searching for a hostname consisting of that string; resulting in an information leak. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/,	A-MOZ-THUN-171220/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26966**	https://www.mozilla.org/security/advisories/mfsa2020-52/	
Out-of-bounds Write	09-Dec-20	9.3	Mozilla developers reported memory safety bugs present in Firefox 82 and Firefox ESR 78.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26968**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	A-MOZ-THUN-171220/402
Out-of-bounds Write	09-Dec-20	9.3	When reading SMTP server status codes, Thunderbird writes an integer value to a position on the stack that is intended to contain just one byte. Depending on processor architecture and stack layout, this leads to stack corruption that may be exploitable. This vulnerability affects Thunderbird < 78.5.1. **CVE ID : CVE-2020-26970**	https://www.mozilla.org/security/advisories/mfsa2020-53/	A-MOZ-THUN-171220/403
mquery_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mquery					
N/A	11-Dec-20	5	lib/utils.js in mquery before 3.2.3 allows a pollution attack because a special property (e.g., __proto__) can be copied during a merge or clone operation. **CVE ID : CVE-2020-35149**	N/A	A-MQU-MQUE-171220/404
multi_restaurant_table_reservation_system_project					
multi_restaurant_table_reservation_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-20	7.5	The file view-chair-list.php in Multi Restaurant Table Reservation System 1.0 does not perform input validation on the table_id parameter which allows unauthenticated SQL Injection. An attacker can send malicious input in the GET request to /dashboard/view-chair-list.php?table_id= to trigger the vulnerability. **CVE ID : CVE-2020-29284**	N/A	A-MUL-MULT-171220/405
Netflix					
chaos_monkey					
Missing Authorization	03-Dec-20	5	Jenkins Chaos Monkey Plugin 0.3 and earlier does not perform permission checks in several HTTP endpoints, allowing attackers with Overall/Read permission to generate load and to generate memory leaks. **CVE ID : CVE-2020-2322**	https://www.jenkins.io/security/advisory/2020-12-03/#SECURITY-2109%20(1)	A-NET-CHAO-171220/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	03-Dec-20	5	Jenkins Chaos Monkey Plugin 0.4 and earlier does not perform permission checks in an HTTP endpoint, allowing attackers with Overall/Read permission to access the Chaos Monkey page and to see the history of actions. **CVE ID : CVE-2020-2323**	https://www.jenkins.io/security/advisory/2020-12-03/#SECURITY-2109%20(2)	A-NET-CHAO-171220/407
Netscout					
airmagnet_enterprise					
Improper Privilege Management	03-Dec-20	9.3	NETSCOUT AirMagnet Enterprise 11.1.4 build 37257 and earlier has a sensor escalated privileges vulnerability that can be exploited to provide someone with administrative access to a sensor, with credentials to invoke a command to provide root access to the operating system. The attacker must complete a straightforward password-cracking exercise. **CVE ID : CVE-2020-28251**	https://www.netscout.com/securityadvisories	A-NET-AIRM-171220/408
Nlnetlabs					
unbound					
Improper Link Resolution Before File Access ('Link Following')	07-Dec-20	2.1	NLnet Labs Unbound, up to and including version 1.12.0, and NLnet Labs NSD, up to and including version 4.3.3, contain a local vulnerability that would allow for a local symlink attack. When writing the PID file,	https://www.nlnetlabs.nl/downloads/nsd/CVE-2020-28935.txt, https://www.nlnetlabs.	A-NLN-UNBO-171220/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Unbound and NSD create the file if it is not there, or open an existing file for writing. In case the file was already present, they would follow symlinks if the file happened to be a symlink instead of a regular file. An additional chown of the file would then take place after it was written, making the user Unbound/NSD is supposed to run as the new owner of the file. If an attacker has local access to the user Unbound/NSD runs as, she could create a symlink in place of the PID file pointing to a file that she would like to erase. If then Unbound/NSD is killed and the PID file is not cleared, upon restarting with root privileges, Unbound/NSD will rewrite any file pointed at by the symlink. This is a local vulnerability that could create a Denial of Service of the system Unbound/NSD is running on. It requires an attacker having access to the limited permission user Unbound/NSD runs as and point through the symlink to a critical file on the system. **CVE ID : CVE-2020-28935**	nl/downloads/unbound/CVE-2020-28935.txt	
name_server_daemon					
Improper Link	07-Dec-20	2.1	NLnet Labs Unbound, up to and including version 1.12.0,	https://www.nlnetlabs.	A-NLN-NAME-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resolution Before File Access ('Link Following')			and NLnet Labs NSD, up to and including version 4.3.3, contain a local vulnerability that would allow for a local symlink attack. When writing the PID file, Unbound and NSD create the file if it is not there, or open an existing file for writing. In case the file was already present, they would follow symlinks if the file happened to be a symlink instead of a regular file. An additional chown of the file would then take place after it was written, making the user Unbound/NSD is supposed to run as the new owner of the file. If an attacker has local access to the user Unbound/NSD runs as, she could create a symlink in place of the PID file pointing to a file that she would like to erase. If then Unbound/NSD is killed and the PID file is not cleared, upon restarting with root privileges, Unbound/NSD will rewrite any file pointed at by the symlink. This is a local vulnerability that could create a Denial of Service of the system Unbound/NSD is running on. It requires an attacker having access to the limited permission user Unbound/NSD runs as and point through the symlink to	nl/downloads/nsd/CVE-2020-28935.txt, https://www.nlnetlabs.nl/downloads/unbound/CVE-2020-28935.txt	171220/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a critical file on the system. **CVE ID : CVE-2020-28935**		
node-notifier_project					
node-notifier					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Dec-20	10	This affects the package node-notifier before 9.0.0. It allows an attacker to run arbitrary commands on Linux machines due to the options params not being sanitised when being passed an array. **CVE ID : CVE-2020-7789**	N/A	A-NOD-NODE-171220/411
notable					
notable					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	9.3	Notable 1.8.4 allows XSS via crafted Markdown text, with resultant remote code execution (because nodeIntegration in webPreferences is true). **CVE ID : CVE-2020-16608**	N/A	A-NOT-NOTA-171220/412
omniauth-apple_project					
omniauth-apple					
Authentication Bypass by Spoofing	08-Dec-20	5	omniauth-apple is the OmniAuth strategy for "Sign In with Apple" (RubyGem omniauth-apple). In omniauth-apple before version 1.0.1 attackers can fake their email address during authentication. This vulnerability impacts applications using the omniauth-apple strategy of OmniAuth and using the	https://github.com/nhosoya/omniauth-apple/security/advisories/GHSA-49r3-2549-3633	A-OMN-OMNI-171220/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			info.email field of OmniAuth's Auth Hash Schema for any kind of identification. The value of this field may be set to any value of the attacker's choice including email addresses of other users. Applications not using info.email for identification but are instead using the uid field are not impacted in the same manner. Note, these applications may still be negatively affected if the value of info.email is being used for other purposes. Applications using affected versions of omniauth-apple are advised to upgrade to omniauth-apple version 1.0.1 or later. **CVE ID : CVE-2020-26254**		
online_bus_booking_system_project_using_php\/mysql_project					
online_bus_booking_system_project_using_php\/mysql					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Dec-20	7.5	Online Bus Booking System Project Using PHP/MySQL version 1.0 has SQL injection via the login page. By placing SQL injection payload on the login page attackers can bypass the authentication and can gain the admin privilege. **CVE ID : CVE-2020-25889**	N/A	A-ONL-ONLI-171220/414
online_bus_ticket_reservation_project					
online_bus_ticket_reservation					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Dec-20	7.5	SQL Injection in the login page in Online Bus Ticket Reservation 1.0 allows attackers to execute arbitrary SQL commands and bypass authentication via the username and password fields. **CVE ID : CVE-2020-35378**	N/A	A-ONL-ONLI-171220/415
online_doctor_appointment_booking_system_php_and_mysql_project					
online_doctor_appointment_booking_system_php_and_mysql					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-20	7.5	An SQL injection vulnerability was discovered in Online Doctor Appointment Booking System PHP and Mysql via the q parameter to getuser.php. **CVE ID : CVE-2020-29283**	N/A	A-ONL-ONLI-171220/416
online_examination_system_project					
online_examination_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	4.3	Cross-site scripting (XSS) vulnerability in Online Examination System 1.0 via the q parameter to feedback.php. **CVE ID : CVE-2020-29257**	N/A	A-ONL-ONLI-171220/417
Improper Neutralization of Input During Web Page Generation ('Cross-site	09-Dec-20	4.3	Cross-site scripting (XSS) vulnerability in Online Examination System 1.0 via the w parameter to index.php. **CVE ID : CVE-2020-29258**	N/A	A-ONL-ONLI-171220/418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	4.3	Cross-site scripting (XSS) vulnerability in Online Examination System 1.0 via the subject or feedback parameter to feedback.php. **CVE ID : CVE-2020-29259**	N/A	A-ONL-ONLI-171220/419
online_voting_system_project					
online_voting_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-20	4.3	Online Birth Certificate System Project V 1.0 is affected by cross-site scripting (XSS). This vulnerability can result in an attacker injecting the XSS payload in the User Registration section. When an admin visits the View Detail of Application section from the admin panel, the attacker can able to steal the cookie according to the crafted payload. **CVE ID : CVE-2020-29239**	N/A	A-ONL-ONLI-171220/420
openasset					
digital_asset_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Dec-20	4.3	OpenAsset Digital Asset Management (DAM) through 12.0.19, does not correctly sanitize user supplied input in multiple parameters and endpoints, allowing for stored cross-site scripting attacks. **CVE ID : CVE-2020-28857**	N/A	A-OPE-DIGI-171220/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	14-Dec-20	6.8	OpenAsset Digital Asset Management (DAM) through 12.0.19 does not correctly verify whether a request made to the application was intentionally made by the user, allowing for cross-site request forgery attacks on all user functions. **CVE ID : CVE-2020-28858**	N/A	A-OPE-DIGI-171220/422
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Dec-20	4.3	OpenAsset Digital Asset Management (DAM) through 12.0.19 does not correctly sanitize user supplied input in multiple parameters and endpoints, allowing for reflected cross-site scripting attacks. **CVE ID : CVE-2020-28859**	N/A	A-OPE-DIGI-171220/423
openclinic_project					
openclinic					
Improper Authentication	03-Dec-20	5	OpenClinic version 0.8.2 is affected by a missing authentication vulnerability that allows unauthenticated users to access any patient's medical test results, possibly resulting in disclosure of Protected Health Information (PHI) stored in the application, via a direct request for the /tests/ URI. **CVE ID : CVE-2020-28937**	N/A	A-OPE-OPEN-171220/424
Improper Neutralization of Input During Web Page	03-Dec-20	3.5	OpenClinic version 0.8.2 is affected by a stored XSS vulnerability in lib/Check.php that allows users of the application to	N/A	A-OPE-OPEN-171220/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			force actions on behalf of other users. **CVE ID : CVE-2020-28938**		
Unrestricted Upload of File with Dangerous Type	03-Dec-20	6.5	OpenClinic version 0.8.2 is affected by a medical/test_new.php insecure file upload vulnerability. This vulnerability allows authenticated users (with substantial privileges) to upload malicious files, such as PHP web shells, which can lead to arbitrary code execution on the application server. **CVE ID : CVE-2020-28939**	N/A	A-OPE-OPEN-171220/426
Openldap					
openldap					
NULL Pointer Dereference	08-Dec-20	5	A NULL pointer dereference was found in OpenLDAP server and was fixed in openldap 2.4.55, during a request for renaming RDNs. An unauthenticated attacker could remotely crash the slapd process by sending a specially crafted request, causing a Denial of Service. **CVE ID : CVE-2020-25692**	https://bugzilla.redhat.com/show_bug.cgi?id=1894567	A-OPE-OPEN-171220/427
Openssl					
openssl					
NULL Pointer Dereference	08-Dec-20	5	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as	https://git.openssl.org/gitweb/?p=openssl.git;a=commitd	A-OPE-OPEN-171220/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download	iff;h=2154ab83e14ede338d2ede9bbe5cdfce5d5a6c9e, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=f960d81215ebf3f65e03d4d5d857fb9b666d6920, https://www.openssl.org/news/secadv/20201208.txt	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w). **CVE ID : CVE-2020-1971**		
Openstack					
horizon					
URL Redirection to Untrusted Site ('Open	04-Dec-20	5.8	An issue was discovered in OpenStack Horizon before 15.3.2, 16.x before 16.2.1, 17.x and 18.x before 18.3.3,	https://security.openstack.org/ossa/OSSA-	A-OPE-HORI-171220/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redirect')			18.4.x, and 18.5.x. There is a lack of validation of the "next" parameter, which would allow someone to supply a malicious URL in Horizon that can cause an automatic redirect to the provided malicious URL. **CVE ID : CVE-2020-29565**	2020-008.html	
os4ed					
opensis					
Inadequate Encryption Strength	04-Dec-20	5	OpenSIS Community Edition through 7.6 is affected by incorrect access controls for the file ResetUserInfo.php that allow an unauthenticated attacker to change the password of arbitrary users. **CVE ID : CVE-2020-27408**	N/A	A-OS4-OPEN-171220/430
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Dec-20	4.3	OpenSIS Community Edition before 7.5 is affected by a cross-site scripting (XSS) vulnerability in SideForStudent.php via the modname parameter. **CVE ID : CVE-2020-27409**	N/A	A-OS4-OPEN-171220/431
Paloaltonetworks					
cortex_xdr_agent					
Improper Handling of Exceptional Conditions	09-Dec-20	2.1	An improper handling of exceptional conditions vulnerability in Cortex XDR Agent allows a local authenticated Windows user to create files in the software's internal program	https://security.paloaltonetworks.com/CVE-2020-2020	A-PAL-CORT-171220/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			directory that prevents the Cortex XDR Agent from starting. The exceptional condition is persistent and prevents Cortex XDR Agent from starting when the software or machine is restarted. This issue impacts: Cortex XDR Agent 5.0 versions earlier than 5.0.10; Cortex XDR Agent 6.1 versions earlier than 6.1.7; Cortex XDR Agent 7.0 versions earlier than 7.0.3; Cortex XDR Agent 7.1 versions earlier than 7.1.2. **CVE ID : CVE-2020-2020**		
papermerge					
papermerge					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-20	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Papermerge before 1.5.2 allow remote attackers to inject arbitrary web script or HTML via the rename, tag, upload, or create folder function. The payload can be in a folder, a tag, or a document's filename. If email consumption is configured in Papermerge, a malicious document can be sent by email and is automatically uploaded into the Papermerge web application. Therefore, no authentication is required to exploit XSS if email consumption is configured.	N/A	A-PAP-PAPE-171220/433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Otherwise authentication is required. **CVE ID : CVE-2020-29456**		
phpldapadmin_project					
phpldapadmin					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	3.5	An XSS issue has been discovered in phpLDAPadmin before 1.2.6.2 that allows users to store malicious values that may be executed by other users at a later time via get_request in lib/function.php. **CVE ID : CVE-2020-35132**	N/A	A-PHP-PHPL-171220/434
phpshe					
phpshe					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Dec-20	7.5	PHPSHE 1.7 has SQL injection via the admin.php?mod=user&userlevel_id=1 userlevel_id[] parameter. **CVE ID : CVE-2020-19165**	N/A	A-PHP-PHPS-171220/435
phpspreadsheet_project					
phpspreadsheet					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	3.5	This affects the package phpoffice/phpspreadsheet from 0.0.0. The library is vulnerable to XSS when creating an html output from an excel file by adding a comment on any cell. The root cause of this issue is within the HTML writer	N/A	A-PHP-PHPS-171220/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			where user comments are concatenated as part of link and this is returned as HTML. A fix for this issue is available on commit 0ed5b800be2136bcb8fa9c1bdf59abc957a98845/master branch. **CVE ID : CVE-2020-7776**		
Pimcore					
pimcore					
Improper Preservation of Permissions	03-Dec-20	4	Pimcore is an open source digital experience platform. In Pimcore before version 6.8.5 it is possible to modify & create website settings without having the appropriate permissions. **CVE ID : CVE-2020-26246**	https://github.com/pimcore/pimcore/security/advisories/GHSA-7p8p-4253-3mg6	A-PIM-PIMC-171220/437
pixar					
openusd					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-20	6.8	A heap overflow vulnerability exists in Pixar OpenUSD 20.05 when the software parses compressed sections in binary USD files. A specially crafted USDC file format path jumps decompression heap overflow in a way path jumps are processed. To trigger this vulnerability, the victim needs to open an attacker-provided malformed file. **CVE ID : CVE-2020-13493**	N/A	A-PIX-OPEN-171220/438
Buffer Copy	02-Dec-20	4.3	A heap overflow	N/A	A-PIX-OPEN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			vulnerability exists in the Pixar OpenUSD 20.05 parsing of compressed string tokens in binary USD files. A specially crafted malformed file can trigger a heap overflow which can result in out of bounds memory access which could lead to information disclosure. This vulnerability could be used to bypass mitigations and aid further exploitation. To trigger this vulnerability, victim needs to access an attacker-provided malformed file. **CVE ID : CVE-2020-13494**		171220/439
Out-of-bounds Read	02-Dec-20	4.3	An exploitable vulnerability exists in the way Pixar OpenUSD 20.05 handles parses certain encoded types. A specially crafted malformed file can trigger an arbitrary out of bounds memory access in TfToken Type Index. This vulnerability could be used to bypass mitigations and aid further exploitation. To trigger this vulnerability, the victim needs to access an attacker-provided malformed file. **CVE ID : CVE-2020-13496**	N/A	A-PIX-OPEN-171220/440
Out-of-bounds Read	02-Dec-20	4.3	An exploitable vulnerability exists in the way Pixar OpenUSD 20.05 handles parses certain encoded	N/A	A-PIX-OPEN-171220/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			types. A specially crafted malformed file can trigger an arbitrary out of bounds memory access in String Type Index. This vulnerability could be used to bypass mitigations and aid further exploitation. To trigger this vulnerability, the victim needs to access an attacker-provided malformed file. **CVE ID : CVE-2020-13497**		
Out-of-bounds Read	02-Dec-20	4.3	An exploitable vulnerability exists in the way Pixar OpenUSD 20.05 handles parses certain encoded types. A specially crafted malformed file can trigger an arbitrary out of bounds memory access in SdfPath Type Index. This vulnerability could be used to bypass mitigations and aid further exploitation. To trigger this vulnerability, the victim needs to access an attacker-provided malformed file. **CVE ID : CVE-2020-13498**	N/A	A-PIX-OPEN-171220/442
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Dec-20	4.3	An out-of-bounds memory corruption vulnerability exists in the way Pixar OpenUSD 20.05 uses SPECS data from binary USD files. A specially crafted malformed file can trigger an out-of-bounds memory access and modification which results in	https://support.apple.com/kb/HT212011	A-PIX-OPEN-171220/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory corruption. To trigger this vulnerability, the victim needs to access an attacker-provided malformed file. **CVE ID : CVE-2020-13524**		
Use After Free	03-Dec-20	6.8	A use-after-free vulnerability exists in a way Pixar OpenUSD 20.08 processes reference paths textual USD files. A specially crafted file can trigger the reuse of a freed memory which can result in further memory corruption and arbitrary code execution. To trigger this vulnerability, the victim needs to open an attacker-provided malformed file. **CVE ID : CVE-2020-13531**	N/A	A-PIX-OPEN-171220/444
point_of_sales_in_php\/pdo_project					
point_of_sales_in_php\/pdo					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-20	7.5	SQL injection vulnerability was discovered in Point of Sales in PHP/PDO 1.0, which can be exploited via the id parameter to edit_category.php. **CVE ID : CVE-2020-29285**	N/A	A-POI-POIN-171220/445
Prestashop					
productcomments					
Improper Neutralization of Special Elements	03-Dec-20	6.4	In the PrestaShop module "productcomments" before version 4.2.1, an attacker can use a Blind SQL injection to	https://github.com/PrestaShop/productcomm	A-PRE-PROD-171220/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			retrieve data or stop the MySQL service. The problem is fixed in 4.2.1 of the module. **CVE ID : CVE-2020-26248**	ents/security/advisories/GHSA-5v44-7647-xfw9	
processmaker					
processmaker					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Dec-20	6.5	The sort parameter in the download page /sysworkflow/en/neoclassic/reportTables/reportTables_Ajax is vulnerable to SQL injection in ProcessMaker 3.4.11. A specially crafted HTTP request can cause an SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-13525**	N/A	A-PRO-PROC-171220/447
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Dec-20	6.5	SQL injection vulnerability exists in the handling of sort parameters in ProcessMaker 3.4.11. A specially crafted HTTP request can cause an SQL injection. The reportTables_Ajax and clientSetupAjax pages are vulnerable to SQL injection in the sort parameter.An attacker can make an authenticated HTTP request to trigger these vulnerabilities. **CVE ID : CVE-2020-13526**	N/A	A-PRO-PROC-171220/448
pytest					
py					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Dec-20	5	A denial of service via regular expression in the py.path.svnwc component of py (aka python-py) through 1.9.0 could be used by attackers to cause a compute-time denial of service attack by supplying malicious input to the blame functionality. **CVE ID : CVE-2020-29651**	N/A	A-PYT-PY-171220/449
python_openid_connect_project					
python_openid_connect					
Improper Verification of Cryptographic Signature	02-Dec-20	4.9	Python oic is a Python OpenID Connect implementation. In Python oic before version 1.2.1, there are several related cryptographic issues affecting client implementations that use the library. The issues are: 1) The IdToken signature algorithm was not checked automatically, but only if the expected algorithm was passed in as a kwarg. 2) JWA `none` algorithm was allowed in all flows. 3) oic.consumer.Consumer.parse_authz returns an unverified IdToken. The verification of the token was left to the discretion of the implementator. 4) iat claim was not checked for sanity (i.e. it could be in the future). These issues are patched in version 1.2.1.	https://github.com/OpenIDC/pyoidc/security/advisories/GHSA-4fjv-pmhg-3rfg	A-PYT-PYTH-171220/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-26244		
Qemu					
qemu					
Reachable Assertion	02-Dec-20	2.1	A reachable assertion issue was found in the USB EHCI emulation code of QEMU. It could occur while processing USB requests due to missing handling of DMA memory map failure. A malicious privileged user within the guest may abuse this flaw to send bogus USB requests and crash the QEMU process on the host, resulting in a denial of service. **CVE ID : CVE-2020-25723**	N/A	A-QEM-QEMU-171220/451
Out-of-bounds Write	08-Dec-20	2.1	A flaw was found in the memory management API of QEMU during the initialization of a memory region cache. This issue could lead to an out-of-bounds write access to the MSI-X table while performing MMIO operations. A guest user may abuse this flaw to crash the QEMU process on the host, resulting in a denial of service. This flaw affects QEMU versions prior to 5.2.0. **CVE ID : CVE-2020-27821**	N/A	A-QEM-QEMU-171220/452
Loop with Unreachable Exit Condition	04-Dec-20	2.1	hw/net/e1000e_core.c in QEMU 5.0.0 has an infinite loop via an RX descriptor with a NULL buffer address.	http://www.openwall.com/lists/oss-	A-QEM-QEMU-171220/453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			**CVE ID : CVE-2020-28916**	security/2020/12/01/2	
Qnap					
multimedia_console					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	4.3	This cross-site scripting vulnerability in Multimedia Console allows remote attackers to inject malicious code. QANP have already fixed this vulnerability in Multimedia Console 1.1.5 and later. **CVE ID : CVE-2020-2493**	https://www.qnap.com/en/security-advisory/qsa-20-14	A-QNA-MULT-171220/454
quts_hero					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	4.3	This cross-site scripting vulnerability in Music Station allows remote attackers to inject malicious code. QANP have already fixed this vulnerability in the following versions of Music Station. QuTS hero h4.5.1: Music Station 5.3.13 and later QTS 4.5.1: Music Station 5.3.12 and later QTS 4.4.3: Music Station 5.3.12 and later **CVE ID : CVE-2020-2494**	https://www.qnap.com/en/security-advisory/qsa-20-13	A-QNA-QUTS-171220/455
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	4.3	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in File Station. QANP have already fixed these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build	https://www.qnap.com/en/security-advisory/qsa-20-12	A-QNA-QUTS-171220/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later **CVE ID : CVE-2020-2495**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	4.3	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in File Station. QANP have already fixed these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later **CVE ID : CVE-2020-2496**	https://www.qnap.com/en/security-advisory/qsa-20-12	A-QNA-QUTS-171220/457
Improper Neutralization of Input During Web Page Generation	10-Dec-20	4.3	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in System Connection Logs. QANP have already fixed	https://www.qnap.com/en/security-advisory/qsa-20-12	A-QNA-QUTS-171220/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later **CVE ID : CVE-2020-2497**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	4.3	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in certificate configuration. QANP have already fixed these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later **CVE ID : CVE-2020-2498**	https://www.qnap.com/en/security-advisory/qsa-20-12	A-QNA-QUTS-171220/459
qts					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	4.3	This cross-site scripting vulnerability in Music Station allows remote attackers to inject malicious code. QANP have already fixed this vulnerability in the following versions of Music Station. QuTS hero h4.5.1: Music Station 5.3.13 and later QTS 4.5.1: Music Station 5.3.12 and later QTS 4.4.3: Music Station 5.3.12 and later **CVE ID : CVE-2020-2494**	https://www.qnap.com/en/security-advisory/qsa-20-13	A-QNA-QTS-171220/460
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	4.3	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in File Station. QANP have already fixed these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later **CVE ID : CVE-2020-2495**	https://www.qnap.com/en/security-advisory/qsa-20-12	A-QNA-QTS-171220/461
Improper Neutralization of Input During Web	10-Dec-20	4.3	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in File	https://www.qnap.com/en/security-	A-QNA-QTS-171220/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			Station. QANP have already fixed these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later **CVE ID : CVE-2020-2496**	advisory/qsa-20-12	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	4.3	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in System Connection Logs. QANP have already fixed these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later **CVE ID : CVE-2020-2497**	https://www.qnap.com/en/security-advisory/qsa-20-12	A-QNA-QTS-171220/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	4.3	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in certificate configuration. QANP have already fixed these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later **CVE ID : CVE-2020-2498**	https://www.qnap.com/en/security-advisory/qsa-20-12	A-QNA-QTS-171220/464
music_station					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	4.3	This cross-site scripting vulnerability in Music Station allows remote attackers to inject malicious code. QANP have already fixed this vulnerability in the following versions of Music Station. QuTS hero h4.5.1: Music Station 5.3.13 and later QTS 4.5.1: Music Station 5.3.12 and later QTS 4.4.3: Music Station 5.3.12 and later **CVE ID : CVE-2020-2494**	https://www.qnap.com/en/security-advisory/qsa-20-13	A-QNA-MUSI-171220/465
photo_station					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	4.3	This cross-site scripting vulnerability in Photo Station allows remote attackers to inject malicious code. QANP We have already fixed this vulnerability in the following versions of Photo Station. QTS 4.5.1: Photo Station 6.0.12 and later QTS 4.4.3: Photo Station 6.0.12 and later QTS 4.3.6: Photo Station 5.7.12 and later QTS 4.3.4: Photo Station 5.7.13 and later QTS 4.3.3: Photo Station 5.4.10 and later QTS 4.2.6: Photo Station 5.2.11 and later **CVE ID : CVE-2020-2491**	https://www.qnap.com/en/security-advisory/qsa-20-15	A-QNA-PHOT-171220/466
react-adal_project					
react-adal					
Improper Authentication	09-Dec-20	5	This affects all versions of package react-adal. It is possible for a specially crafted JWT token and request URL can cause the nonce, session and refresh values to be incorrectly validated, causing the application to treat an attacker-generated JWT token as authentic. The logical defect is caused by how the nonce, session and refresh values are stored in the browser local storage or session storage. Each key is automatically appended by ||. When the received nonce and session keys are	N/A	A-REA-REAC-171220/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			generated, the list of values is stored in the browser storage, separated by ||, with || always appended to the end of the list. Since || will always be the last 2 characters of the stored values, an empty string ("") will always be in the list of the valid values. Therefore, if an empty session parameter is provided in the callback URL, and a specially-crafted JWT token contains an nonce value of "" (empty string), then adal.js will consider the JWT token as authentic. **CVE ID : CVE-2020-7787**		
Redhat					
wildfly					
Improper Release of Memory Before Removing Last Reference	08-Dec-20	7.1	A flaw was found in Wildfly affecting versions 19.0.0.Final, 19.1.0.Final, 20.0.0.Final, 20.0.1.Final, and 21.0.0.Final. When an application uses the OpenTracing API's java-interceptors, there is a possibility of a memory leak. This flaw allows an attacker to impact the availability of the server. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-27822**	https://bugzilla.redhat.com/show_bug.cgi?id=1904060	A-RED-WILD-171220/468
software_collections					
Improper	03-Dec-20	4.3	A XSS vulnerability was	N/A	A-RED-SOFT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			discovered in python-lxml's clean module. The module's parser didn't properly imitate browsers, which caused different behaviors between the sanitizer and the user's page. A remote attacker could exploit this flaw to run arbitrary HTML/JS code. **CVE ID : CVE-2020-27783**		171220/469
storage					
Improper Privilege Management	03-Dec-20	4	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker. **CVE ID : CVE-2020-14318**	N/A	A-RED-STOR-171220/470
cloudforms					
Cross-Site Request Forgery (CSRF)	02-Dec-20	6.8	This release fixes a Cross Site Request Forgery vulnerability was found in Red Hat CloudForms which forces end users to execute unwanted actions on a web application in which the user is currently authenticated. An attacker can make a forgery HTTP request to the server by crafting custom flash file which can force the user to perform state changing requests like provisioning VMs, running	N/A	A-RED-CLOU-171220/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ansible playbooks and so forth. **CVE ID : CVE-2020-14369**		
data_grid					
Improper Privilege Management	03-Dec-20	4.9	A flaw was found in infinispan 10 REST API, where authorization permissions are not checked while performing some server management operations. When authz is enabled, any user with authentication can perform operations like shutting down the server without the ADMIN role. **CVE ID : CVE-2020-25711**	N/A	A-RED-DATA-171220/472
openshift_container_platform					
Use After Free	11-Dec-20	7.2	A flaw was found in the Linux kernels implementation of MIDI (kernel 5.7-rc6), where an attacker with a local account and the permissions to issue an ioctl commands to midi devices, could trigger a use-after-free. A write to this specific memory while freed and before use could cause the flow of execution to change and possibly allow for memory corruption or privilege escalation. **CVE ID : CVE-2020-27786**	N/A	A-RED-OPEN-171220/473
URL Redirection to Untrusted Site ('Open	02-Dec-20	5.8	The elasticsearch-operator does not validate the namespace where kibana logging resource is created	N/A	A-RED-OPEN-171220/474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redirect')			and due to that it is possible to replace the original openshift-logging console link (kibana console) to different one, created based on the new CR for the new kibana resource. This could lead to an arbitrary URL redirection or the openshift-logging console link damage. This flaw affects elasticsearch-operator-container versions before 4.7. **CVE ID : CVE-2020-27816**		
libvirt					
Missing Release of Resource after Effective Lifetime	03-Dec-20	7.2	A flaw was found in libvirt, where it leaked a file descriptor for `/dev/mapper/control` into the QEMU process. This file descriptor allows for privileged operations to happen against the device-mapper on the host. This flaw allows a malicious guest user or process to perform operations outside of their standard permissions, potentially causing serious damage to the host operating system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2020-14339**	N/A	A-RED-LIBV-171220/475
enterprise_mrg					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	11-Dec-20	7.2	A flaw was found in the Linux kernels implementation of MIDI (kernel 5.7-rc6), where an attacker with a local account and the permissions to issue an ioctl commands to midi devices, could trigger a use-after-free. A write to this specific memory while freed and before use could cause the flow of execution to change and possibly allow for memory corruption or privilege escalation. **CVE ID : CVE-2020-27786**	N/A	A-RED-ENTE-171220/476
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Dec-20	5.4	A use-after-free flaw was found in kernel/trace/ring_buffer.c in Linux kernel (before 5.10-rc1). There was a race problem in trace_open and resize of cpu buffer running parallely on different cpus, may cause a denial of service problem (DOS). This flaw could even allow a local attacker with special user privilege to a kernel information leak threat. **CVE ID : CVE-2020-27825**	N/A	A-RED-ENTE-171220/477
ceph_storage					
Cleartext Storage of Sensitive Information	08-Dec-20	2.1	Ceph-ansible 4.0.34.1 creates /etc/ceph/iscsi-gateway.conf with insecure default permissions, allowing any user to read the sensitive information within.	https://bugzilla.redhat.com/show_bug.cgi?id=1892108, https://github.com/cep	A-RED-CEPH-171220/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-25677	h/ceph-ansible/pull/5964	
saibo					
cyber_game_accelerator					
Improper Privilege Management	03-Dec-20	4.6	In Saibo Cyber Game Accelerator 3.7.9 there is a local privilege escalation vulnerability. Attackers can use the constructed program to increase user privileges **CVE ID : CVE-2020-23735**	N/A	A-SAI-CYBE-171220/479
Samba					
samba					
Improper Privilege Management	03-Dec-20	4	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker. **CVE ID : CVE-2020-14318**	N/A	A-SAM-SAMB-171220/480
N/A	02-Dec-20	4	A flaw was found in samba's DNS server. An authenticated user could use this flaw to the RPC server to crash. This RPC server, which also serves protocols other than dnsserver, will be restarted after a short delay, but it is easy for an authenticated non administrative attacker to crash it again as soon as it returns. The Samba DNS	N/A	A-SAM-SAMB-171220/481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server itself will continue to operate, but many RPC services will not. **CVE ID : CVE-2020-14383**		
SAP					
s\/4_hana					
Missing Authorization	09-Dec-20	7.5	SAP AS ABAP (SAP Landscape Transformation), versions - 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020 and SAP S4 HANA (SAP Landscape Transformation), versions - 101, 102, 103, 104, 105, allows a high privileged user to execute a RFC function module to which access should be restricted, however due to missing authorization an attacker can get access to some sensitive internal information of vulnerable SAP system or to make vulnerable SAP systems completely unavailable. **CVE ID : CVE-2020-26832**	N/A	A-SAP-S\/4-171220/482
hana_database					
Improper Authentication	09-Dec-20	5.5	SAP HANA Database, version - 2.0, does not correctly validate the username when performing SAML bearer token-based user authentication. It is possible to manipulate a valid existing SAML bearer token to authenticate as a user	N/A	A-SAP-HANA-171220/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			whose name is identical to the truncated username for whom the SAML bearer token was issued. **CVE ID : CVE-2020-26834**		
business_warehouse					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-20	9	SAP Business Warehouse, versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 782, and SAP BW4HANA, versions - 100, 200 allows an attacker authenticated with (high) developer privileges to submit a crafted request to generate and execute code without requiring any user interaction. It is possible to craft a request which will result in the execution of Operating System commands leading to Code Injection vulnerability which could completely compromise the confidentiality, integrity and availability of the server and any data or other applications running on it. **CVE ID : CVE-2020-26838**	N/A	A-SAP-BUSI-171220/484
solution_manager					
Missing Authorization	09-Dec-20	5.5	SAP Solution Manager 7.2 (User Experience Monitoring), version - 7.2, does not perform necessary authorization checks for an authenticated user. Due to inadequate access control, a	N/A	A-SAP-SOLU-171220/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network attacker authenticated as a regular user can use operations which should be restricted to administrators. These operations can be used to Change the User Experience Monitoring configuration, obtain details about the configured SAP Solution Manager agents, Deploy a malicious User Experience Monitoring script. **CVE ID : CVE-2020-26830**		
URL Redirection to Untrusted Site ('Open Redirect')	09-Dec-20	5.8	SAP Solution Manager (Trace Analysis), version - 720, allows for misuse of a parameter in the application URL leading to Open Redirect vulnerability, an attacker can enter a link to malicious site which could trick the user to enter credentials or download malicious software, as a parameter in the application URL and share it with the end user who could potentially become a victim of the attack. **CVE ID : CVE-2020-26836**	N/A	A-SAP-SOLU-171220/486
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Dec-20	6.5	SAP Solution Manager 7.2 (User Experience Monitoring), version - 7.2, allows an authenticated user to upload a malicious script that can exploit an existing path traversal vulnerability to compromise	N/A	A-SAP-SOLU-171220/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			confidentiality exposing elements of the file system, partially compromise integrity allowing the modification of some configurations and partially compromise availability by making certain services unavailable. **CVE ID : CVE-2020-26837**		
disclosure_management					
Unrestricted Upload of File with Dangerous Type	09-Dec-20	5.5	SAP Disclosure Management, version - 10.1, provides capabilities for authorized users to upload and download content of specific file type. In some file types it is possible to enter formulas which can call external applications or execute scripts. The execution of a payload (script) on target machine could be used to steal and modify the data available in the spreadsheet **CVE ID : CVE-2020-26828**	N/A	A-SAP-DISC-171220/488
bw\/4hana					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-20	9	SAP Business Warehouse, versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 782, and SAP BW4HANA, versions - 100, 200 allows an attacker authenticated with (high) developer privileges to submit a crafted request to generate and execute code without requiring any user	N/A	A-SAP-BW\/-171220/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction. It is possible to craft a request which will result in the execution of Operating System commands leading to Code Injection vulnerability which could completely compromise the confidentiality, integrity and availability of the server and any data or other applications running on it. **CVE ID : CVE-2020-26838**		
netweaver_application_server_java					
Missing Encryption of Sensitive Data	09-Dec-20	2.7	SAP AS JAVA (Key Storage Service), versions - 7.10, 7.11, 7.20 ,7.30, 7.31, 7.40, 7.50, has the key material which is stored in the SAP NetWeaver AS Java Key Storage service stored in the database in the DER encoded format and is not encrypted. This enables an attacker who has administrator access to the SAP NetWeaver AS Java to decode the keys because of missing encryption and get some application data and client credentials of adjacent systems. This highly impacts Confidentiality as information disclosed could contain client credentials of adjacent systems. **CVE ID : CVE-2020-26816**	N/A	A-SAP-NETW-171220/490
Unrestricted Upload of	09-Dec-20	4	Process Integration Monitoring of SAP	N/A	A-SAP-NETW-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			NetWeaver AS JAVA, versions - 7.31, 7.40, 7.50, allows an attacker to upload any file (including script files) without proper file format validation, leading to Unrestricted File Upload. **CVE ID : CVE-2020-26826**		171220/491
Improper Authentication	09-Dec-20	9	SAP NetWeaver AS JAVA (P2P Cluster Communication), versions - 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows arbitrary connections from processes because of missing authentication check, that are outside the cluster and even outside the network segment dedicated for the internal cluster communication. As result, an unauthenticated attacker can invoke certain functions that would otherwise be restricted to system administrators only, including access to system administration functions or shutting down the system completely. **CVE ID : CVE-2020-26829**	N/A	A-SAP-NETW-171220/492
netweaver_as_abap					
Missing Authorization	09-Dec-20	7.5	SAP AS ABAP (SAP Landscape Transformation), versions - 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020 and SAP S4 HANA (SAP	N/A	A-SAP-NETW-171220/493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Landscape Transformation), versions - 101, 102, 103, 104, 105, allows a high privileged user to execute a RFC function module to which access should be restricted, however due to missing authorization an attacker can get access to some sensitive internal information of vulnerable SAP system or to make vulnerable SAP systems completely unavailable. **CVE ID : CVE-2020-26832**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-20	4.3	SAP NetWeaver AS ABAP, versions - 740, 750, 751, 752, 753, 754 , does not sufficiently encode URL which allows an attacker to input malicious java script in the URL which could be executed in the browser resulting in Reflected Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2020-26835**	N/A	A-SAP-NETW-171220/494
businessobjects_business_intelligence_platform					
N/A	09-Dec-20	5.5	SAP BusinessObjects BI Platform (Crystal Report), versions - 4.1, 4.2, 4.3, does not sufficiently validate uploaded XML entities during crystal report generation due to missing XML validation, An attacker with basic privileges can inject some arbitrary XML entities leading to internal	N/A	A-SAP-BUSI-171220/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file disclosure, internal directories disclosure, Server-Side Request Forgery (SSRF) and denial-of-service (DoS). **CVE ID : CVE-2020-26831**		
Schneider-electric					
somachine					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Dec-20	5.2	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Modicon M258 Firmware (All versions prior to V5.0.4.11) and SoMachine/SoMachine Motion software (All versions), that could cause a buffer overflow when the length of a file transferred to the webserver is not verified. **CVE ID : CVE-2020-28220**	https://www.se.com/ww/en/download/document/SEVD-2020-343-09/	A-SCH-SOMA-171220/496
somachine_motion					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Dec-20	5.2	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Modicon M258 Firmware (All versions prior to V5.0.4.11) and SoMachine/SoMachine Motion software (All versions), that could cause a buffer overflow when the length of a file transferred to the webserver is not verified.	https://www.se.com/ww/en/download/document/SEVD-2020-343-09/	A-SCH-SOMA-171220/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-28220		
ecostruxure_control_expert					
Write-what-where Condition	11-Dec-20	6.8	A CWE-123: Write-what-where Condition vulnerability exists in EcoStruxure™ Control Expert (all versions) and Unity Pro (former name of EcoStruxure™ Control Expert) (all versions), that could cause a crash of the software or unexpected code execution when opening a malicious file in EcoStruxure™ Control Expert software. **CVE ID : CVE-2020-7560**	https://www.se.com/ww/en/download/document/SEVD-2020-343-01/	A-SCH-ECOS-171220/498
unity_pro					
Write-what-where Condition	11-Dec-20	6.8	A CWE-123: Write-what-where Condition vulnerability exists in EcoStruxure™ Control Expert (all versions) and Unity Pro (former name of EcoStruxure™ Control Expert) (all versions), that could cause a crash of the software or unexpected code execution when opening a malicious file in EcoStruxure™ Control Expert software. **CVE ID : CVE-2020-7560**	https://www.se.com/ww/en/download/document/SEVD-2020-343-01/	A-SCH-UNIT-171220/499
ecostruxure_energy_expert					
Improper Access Control	01-Dec-20	6.5	A CWE-284:Improper Access Control vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power	N/A	A-SCH-ECOS-171220/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Monitoring and SCADA Software (see security notification for version information) that could allow for arbitrary code execution on the server when an authorized user access an affected webpage. **CVE ID : CVE-2020-7545**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-20	3.5	A CWE-79: Improper Neutralization of Input During Web Page Generation vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could allow an attacker to perform actions on behalf of the authorized user when accessing an affected webpage. **CVE ID : CVE-2020-7546**	N/A	A-SCH-ECOS-171220/501
Improper Access Control	01-Dec-20	6.5	A CWE-284: Improper Access Control vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could allow a user the ability to perform actions via the web interface at a higher privilege level. **CVE ID : CVE-2020-7547**	N/A	A-SCH-ECOS-171220/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ecostruxure_power_monitoring_expert					
Improper Access Control	01-Dec-20	6.5	A CWE-284:Improper Access Control vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could allow for arbitrary code execution on the server when an authorized user access an affected webpage. **CVE ID : CVE-2020-7545**	N/A	A-SCH-ECOS-171220/503
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-20	3.5	A CWE-79: Improper Neutralization of Input During Web Page Generation vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could allow an attacker to perform actions on behalf of the authorized user when accessing an affected webpage. **CVE ID : CVE-2020-7546**	N/A	A-SCH-ECOS-171220/504
Improper Access Control	01-Dec-20	6.5	A CWE-284: Improper Access Control vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could allow a user the ability to	N/A	A-SCH-ECOS-171220/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			perform actions via the web interface at a higher privilege level. **CVE ID : CVE-2020-7547**		
power_manager					
Improper Access Control	01-Dec-20	6.5	A CWE-284:Improper Access Control vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could allow for arbitrary code execution on the server when an authorized user access an affected webpage. **CVE ID : CVE-2020-7545**	N/A	A-SCH-POWE-171220/506
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-20	3.5	A CWE-79: Improper Neutralization of Input During Web Page Generation vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could allow an attacker to perform actions on behalf of the authorized user when accessing an affected webpage. **CVE ID : CVE-2020-7546**	N/A	A-SCH-POWE-171220/507
Improper Access Control	01-Dec-20	6.5	A CWE-284: Improper Access Control vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power	N/A	A-SCH-POWE-171220/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Monitoring and SCADA Software (see security notification for version information) that could allow a user the ability to perform actions via the web interface at a higher privilege level. **CVE ID : CVE-2020-7547**		
powerscada_expert_with_advanced_reporting_and_dashboards					
Improper Access Control	01-Dec-20	6.5	A CWE-284:Improper Access Control vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could allow for arbitrary code execution on the server when an authorized user access an affected webpage. **CVE ID : CVE-2020-7545**	N/A	A-SCH-POWE-171220/509
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-20	3.5	A CWE-79: Improper Neutralization of Input During Web Page Generation vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could allow an attacker to perform actions on behalf of the authorized user when accessing an affected webpage.	N/A	A-SCH-POWE-171220/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7546		
Improper Access Control	01-Dec-20	6.5	A CWE-284: Improper Access Control vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could allow a user the ability to perform actions via the web interface at a higher privilege level. **CVE ID : CVE-2020-7547**	N/A	A-SCH-POWE-171220/511
powerscada_operation_with_advanced_reporting_and_dashboards					
Improper Access Control	01-Dec-20	6.5	A CWE-284:Improper Access Control vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could allow for arbitrary code execution on the server when an authorized user access an affected webpage. **CVE ID : CVE-2020-7545**	N/A	A-SCH-POWE-171220/512
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-20	3.5	A CWE-79: Improper Neutralization of Input During Web Page Generation vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could	N/A	A-SCH-POWE-171220/513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to perform actions on behalf of the authorized user when accessing an affected webpage. **CVE ID : CVE-2020-7546**		
Improper Access Control	01-Dec-20	6.5	A CWE-284: Improper Access Control vulnerability exists in EcoStruxure[a] and SmartStruxure[a] Power Monitoring and SCADA Software (see security notification for version information) that could allow a user the ability to perform actions via the web interface at a higher privilege level. **CVE ID : CVE-2020-7547**	N/A	A-SCH-POWE-171220/514
Seeddms					
seeddms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-20	4.3	Cross-site scripting (XSS) exists in SeedDMS 6.0.13 via the folderid parameter to views/bootstrap/class.DropFolderChooser.php. **CVE ID : CVE-2020-28727**	https://sourceforge.net/p/seeddms/code/ci/32b03b1e5880e2f38cecf4ac7743f8f62f33043f/	A-SEE-SEED-171220/515
set-in_project					
set-in					
N/A	02-Dec-20	7.5	Prototype pollution vulnerability in 'set-in' versions 1.0.0 through 2.0.0 allows attacker to cause a denial of service and may lead to remote code	N/A	A-SET-SET--171220/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-28273**		
smartystreets					
liveaddressplugin.js					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	4.3	A cross-Site Scripting (XSS) vulnerability in this.showInvalid and this.showInvalidCountry in SmartyStreets liveAddressPlugin.js 3.2 allows remote attackers to inject arbitrary web script or HTML via any address parameter (e.g., street or country). **CVE ID : CVE-2020-29455**	N/A	A-SMA-LIVE-171220/517
spatie					
browsershot					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	This affects the package spatie/browsershot from 0.0.0. By specifying a URL in the file:// protocol an attacker is able to include arbitrary files in the resultant PDF. **CVE ID : CVE-2020-7790**	N/A	A-SPA-BROW-171220/518
student_management_system_project_in_php_project					
student_management_system_project_in_php					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-20	3.5	SourceCodester Student Management System Project in PHP version 1.0 is vulnerable to stored a cross-site scripting (XSS) via the 'add subject' tab. **CVE ID : CVE-2020-25955**	N/A	A-STU-STUD-171220/519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
systransoft					
pure_neural_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-20	3.5	A Cross-Site Scripting (XSS) issue in WebUI Translation in Systran Pure Neural Server before 9.7.0 allows a threat actor to have a remote authenticated user run JavaScript from a malicious site. **CVE ID : CVE-2020-29539**	N/A	A-SYS-PURE-171220/520
Uncontrolled Resource Consumption	08-Dec-20	5	API calls in the Translation API feature in Systran Pure Neural Server before 9.7.0 allow a threat actor to use the Systran Pure Neural Server as a Denial-of-Service proxy by sending a large amount of translation requests to a destination host on any given TCP port regardless of whether a web service is running on the destination port. **CVE ID : CVE-2020-29540**	N/A	A-SYS-PURE-171220/521
tarsnap					
spiped_docker					
N/A	08-Dec-20	10	The official spiped docker images before 1.5-alpine contain a blank password for a root user. Systems using the spiped docker container deployed by affected versions of the docker image may allow an remote attacker to achieve root access with a blank	N/A	A-TAR-SPIP-171220/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			password. **CVE ID : CVE-2020-29581**		
tensorflow					
tensorflow					
Out-of-bounds Read	10-Dec-20	4.3	In affected versions of TensorFlow the tf.raw_ops.DataFormatVecPermute API does not validate the src_format and dst_format attributes. The code assumes that these two arguments define a permutation of NHWC. This can result in uninitialized memory accesses, read outside of bounds and even crashes. This is fixed in versions 1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, and 2.4.0. **CVE ID : CVE-2020-26267**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-c9f3-9wfr-wgh7	A-TEN-TENS-171220/523
Out-of-bounds Read	10-Dec-20	5	In TensorFlow release candidate versions 2.4.0rc*, the general implementation for matching filesystem paths to globbing pattern is vulnerable to an access out of bounds of the array holding the directories. There are multiple invariants and preconditions that are assumed by the parallel implementation of GetMatchingPaths but are not verified by the PRs introducing it (#40861 and #44310). Thus, we are completely rewriting the implementation to fully	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9jjw-hf72-3mxw	A-TEN-TENS-171220/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specify and validate these. This is patched in version 2.4.0. This issue only impacts master branch and the release candidates for TF version 2.4. The final release of the 2.4 release will be patched. **CVE ID : CVE-2020-26269**		
Textpattern					
textpattern					
Cross-Site Request Forgery (CSRF)	02-Dec-20	6.8	Textpattern CMS 4.6.2 allows CSRF via the prefs subsystem. **CVE ID : CVE-2020-29458**	N/A	A-TEX-TEXT-171220/525
Tiki					
tikiwiki_cms\/groupware					
Cross-Site Request Forgery (CSRF)	11-Dec-20	6.8	TikiWiki 21.2 allows templates to be edited without CSRF protection. This could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected system. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected system. An attacker could exploit this vulnerability by persuading a user of the interface to follow a maliciously crafted link. A successful exploit could allow the attacker to perform arbitrary actions on	N/A	A-TIK-TIKI-171220/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected system with the privileges of the user. These action include allowing attackers to submit their own code through an authenticated user resulting in local file Inclusion. If an authenticated user who is able to edit TikiWiki templates visits an malicious website, template code can be edited. **CVE ID : CVE-2020-29254**		
Trendmicro					
apex_one					
Information Exposure	01-Dec-20	5	An improper access control information disclosure vulnerability in Trend Micro Apex One and OfficeScan XG SP1 could allow an unauthenticated user to connect to the product server and reveal the total agents managed by the server. **CVE ID : CVE-2020-28573**	N/A	A-TRE-APEX-171220/527
Information Exposure	01-Dec-20	5	An improper access control information disclosure vulnerability in Trend Micro Apex One and OfficeScan XG SP1 could allow an unauthenticated user to connect to the product server and reveal version and build information. **CVE ID : CVE-2020-28576**	N/A	A-TRE-APEX-171220/528
Information	01-Dec-20	5	An improper access control information disclosure	N/A	A-TRE-APEX-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			vulnerability in Trend Micro Apex One and OfficeScan XG SP1 could allow an unauthenticated user to connect to the product server and reveal server hostname and db names. **CVE ID : CVE-2020-28577**		171220/529
Information Exposure	01-Dec-20	5	An improper access control information disclosure vulnerability in Trend Micro Apex One and OfficeScan XG SP1 could allow an unauthenticated user to connect to the product server and reveal number of managed agents. **CVE ID : CVE-2020-28582**	N/A	A-TRE-APEX-171220/530
Information Exposure	01-Dec-20	5	An improper access control information disclosure vulnerability in Trend Micro Apex One and OfficeScan XG SP1 could allow an unauthenticated user to connect to the product server and reveal version, build and patch information. **CVE ID : CVE-2020-28583**	N/A	A-TRE-APEX-171220/531
officescan					
Information Exposure	01-Dec-20	5	An improper access control information disclosure vulnerability in Trend Micro Apex One and OfficeScan XG SP1 could allow an unauthenticated user to connect to the product server and reveal the total agents managed by the	N/A	A-TRE-OFFI-171220/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server. **CVE ID : CVE-2020-28573**		
Information Exposure	01-Dec-20	5	An improper access control information disclosure vulnerability in Trend Micro Apex One and OfficeScan XG SP1 could allow an unauthenticated user to connect to the product server and reveal version and build information. **CVE ID : CVE-2020-28576**	N/A	A-TRE-OFFI-171220/533
Information Exposure	01-Dec-20	5	An improper access control information disclosure vulnerability in Trend Micro Apex One and OfficeScan XG SP1 could allow an unauthenticated user to connect to the product server and reveal server hostname and db names. **CVE ID : CVE-2020-28577**	N/A	A-TRE-OFFI-171220/534
Information Exposure	01-Dec-20	5	An improper access control information disclosure vulnerability in Trend Micro Apex One and OfficeScan XG SP1 could allow an unauthenticated user to connect to the product server and reveal number of managed agents. **CVE ID : CVE-2020-28582**	N/A	A-TRE-OFFI-171220/535
Information Exposure	01-Dec-20	5	An improper access control information disclosure vulnerability in Trend Micro Apex One and OfficeScan XG SP1 could allow an unauthenticated user to	N/A	A-TRE-OFFI-171220/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connect to the product server and reveal version, build and patch information. **CVE ID : CVE-2020-28583**		
serverprotect					
Out-of-bounds Write	01-Dec-20	4.6	A heap-based buffer overflow privilege escalation vulnerability in Trend Micro ServerProtect for Linux 3.0 may allow an attacker to escalate privileges on affected installations. An attacker must first obtain the ability to execute high-privileged code on the target in order to exploit this vulnerability. **CVE ID : CVE-2020-28575**	N/A	A-TRE-SERV-171220/537
txjia					
imcat					
Unrestricted Upload of File with Dangerous Type	09-Dec-20	6.5	imcat 5.2 allows an authenticated file upload and consequently remote code execution via the picture functionality. **CVE ID : CVE-2020-23520**	N/A	A-TXJ-IMCA-171220/538
typesettercms					
typesetter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-20	3.5	** DISPUTED ** Typesetter CMS 5.x through 5.1 allows admins to conduct Site Title persistent XSS attacks via an Admin/Configuration URI. NOTE: the significance of this report is disputed because "admins are	N/A	A-TYP-TYPE-171220/539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			considered trustworthy." **CVE ID : CVE-2020-35126**		
ubilling					
ubilling					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-20	10	Ubilling v1.0.9 allows Remote Command Execution as Root user by executing a malicious command that is injected inside the config file and being triggered by another part of the software. **CVE ID : CVE-2020-29311**	N/A	A-UBI-UBIL-171220/540
Umbraco					
umbraco_cms					
Incorrect Permission Assignment for Critical Resource	02-Dec-20	4	Editors/LogViewerController.cs in Umbraco through 8.9.1 allows a user to visit a logviewer endpoint even if they lack Applications.Settings access. **CVE ID : CVE-2020-29454**	N/A	A-UMB-UMBR-171220/541
Valvesoftware					
game_networking_sockets					
Out-of-bounds Write	03-Dec-20	7.5	Valve's Game Networking Sockets prior to version v1.2.0 improperly handles long unreliable segments in function SNP_ReceiveUnreliableSegment() when configured to support plain-text messages, leading to a Heap-Based Buffer Overflow and resulting in a memory corruption and possibly even a remote code	N/A	A-VAL-GAME-171220/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-6017**		
Out-of-bounds Write	02-Dec-20	7.5	Valve's Game Networking Sockets prior to version v1.2.0 improperly handles long encrypted messages in function AES_GCM_DecryptContext::Decrypt() when compiled using libsodium, leading to a Stack-Based Buffer Overflow and resulting in a memory corruption and possibly even a remote code execution. **CVE ID : CVE-2020-6018**	N/A	A-VAL-GAME-171220/543
victor_cms_project					
victor_cms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-20	7.5	The Victor CMS v1.0 application is vulnerable to SQL injection via the 'search' parameter on the search.php page. **CVE ID : CVE-2020-29280**	N/A	A-VIC-VICT-171220/544
Webkitgtk					
webkitgtk					
Use After Free	03-Dec-20	6.8	A code execution vulnerability exists in the WebSocket functionality of Webkit WebKitGTK 2.30.0. A specially crafted web page can trigger a use-after-free vulnerability which can lead to remote code execution. An	N/A	A-WEB-WEBK-171220/545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can get a user to visit a webpage to trigger this vulnerability. **CVE ID : CVE-2020-13543**		
Use After Free	03-Dec-20	6.8	An exploitable use-after-free vulnerability exists in WebKitGTK browser version 2.30.1 x64. A specially crafted HTML web page can cause a use-after-free condition, resulting in a remote code execution. The victim needs to visit a malicious web site to trigger this vulnerability. **CVE ID : CVE-2020-13584**	N/A	A-WEB-WEBK-171220/546
We-con					
plc_editor					
Out-of-bounds Write	01-Dec-20	6.8	WECON PLC Editor Versions 1.3.8 and prior has a stack-based buffer overflow vulnerability has been identified that may allow arbitrary code execution. **CVE ID : CVE-2020-25177**	N/A	A-WE--PLC_-171220/547
Out-of-bounds Read	01-Dec-20	6.8	WECON PLC Editor Versions 1.3.8 and prior has a heap-based buffer overflow vulnerabilities have been identified that may allow arbitrary code execution. **CVE ID : CVE-2020-25181**	N/A	A-WE--PLC_-171220/548
weseek					
growi					
Information Exposure	03-Dec-20	5	GROWI v4.1.3 and earlier allow remote attackers to	N/A	A-WES-GROW-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtain information which is not allowed to access via unspecified vectors. **CVE ID : CVE-2020-5676**		171220/549
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Dec-20	4.3	Reflected cross-site scripting vulnerability in GROWI v4.0.0 and earlier allows remote attackers to inject arbitrary script via unspecified vectors. **CVE ID : CVE-2020-5677**	N/A	A-WES-GROW-171220/550
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Dec-20	4.3	Stored cross-site scripting vulnerability in GROWI v3.8.1 and earlier allows remote attackers to inject arbitrary script via unspecified vectors. **CVE ID : CVE-2020-5678**	N/A	A-WES-GROW-171220/551
westerndigital					
dashboard					
Uncontrolled Search Path Element	12-Dec-20	6.9	Western Digital Dashboard before 3.2.2.9 allows DLL Hijacking that leads to compromise of the SYSTEM account. **CVE ID : CVE-2020-29654**	https://www.westerndigital.com/support/productsecurity/wdc-20011-western-digital-dashboard-privilege-escalation	A-WES-DASH-171220/552
Wireshark					
wireshark					
Improper	11-Dec-20	5	Memory leak in Kafka	https://gitl	A-WIR-WIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Release of Memory Before Removing Last Reference			protocol dissector in Wireshark 3.4.0 and 3.2.0 to 3.2.8 allows denial of service via packet injection or crafted capture file. **CVE ID : CVE-2020-26418**	ab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26418.json	171220/553
Improper Release of Memory Before Removing Last Reference	11-Dec-20	5	Memory leak in the dissection engine in Wireshark 3.4.0 allows denial of service via packet injection or crafted capture file. **CVE ID : CVE-2020-26419**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26419.json	A-WIR-WIRE-171220/554
Improper Release of Memory Before Removing Last Reference	11-Dec-20	5	Memory leak in RTPS protocol dissector in Wireshark 3.4.0 and 3.2.0 to 3.2.8 allows denial of service via packet injection or crafted capture file. **CVE ID : CVE-2020-26420**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26420.json	A-WIR-WIRE-171220/555
Out-of-bounds Read	11-Dec-20	5	Crash in USB HID protocol dissector and possibly other dissectors in Wireshark 3.4.0 and 3.2.0 to 3.2.8 allows denial of service via packet injection or crafted capture file. **CVE ID : CVE-2020-26421**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26421.json	A-WIR-WIRE-171220/556
wisecleaner					
wise_care_365					
N/A	03-Dec-20	4.9	There is a local denial of service vulnerability in Wise Care 365 5.5.4, attackers can cause computer crash (BSOD).	N/A	A-WIS-WISE-171220/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-23726		
ZNC					
znc_docker					
N/A	08-Dec-20	10	The official znc docker images before 1.7.1-slim contain a blank password for a root user. Systems using the znc docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-29577**	N/A	A-ZNC-ZNC_-171220/558
zx2c4					
password-store					
Improper Authenticati on	09-Dec-20	5	pass through 1.7.3 has a possibility of using a password for an unintended resource. For exploitation to occur, the user must do a git pull, decrypt a password, and log into a remote service with the password. If an attacker controls the central Git server or one of the other members' machines, and also controls one of the services already in the password store, they can rename one of the password files in the Git repository to something else: pass doesn't correctly verify that the content of a file matches the filename, so a user might be tricked into decrypting the	N/A	A-ZX2-PASS-171220/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			wrong password and sending that to a service that the attacker controls. NOTE: for environments in which this threat model is of concern, signing commits can be a solution. **CVE ID : CVE-2020-28086**		
Operating System					
Apple					
macos					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-20	4.3	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Big Sur 11.0.1. Processing a maliciously crafted document may lead to a cross site scripting attack. **CVE ID : CVE-2020-10012**	https://support.apple.com/kb/HT212011	O-APP-MACO-171220/560
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-20	4.3	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Big Sur 11.0.1. A malicious application may be able to break out of its sandbox. **CVE ID : CVE-2020-10014**	https://support.apple.com/kb/HT212011	O-APP-MACO-171220/561
N/A	08-Dec-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. An application may be able	https://support.apple.com/kb/HT212011	O-APP-MACO-171220/562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-10016**		
Unchecked Return Value	08-Dec-20	4.3	A denial of service issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.0.1. An attacker may be able to bypass Managed Frame Protection. **CVE ID : CVE-2020-27898**	https://support.apple.com/kb/HT212011	O-APP-MACO-171220/563
Information Exposure	08-Dec-20	4.3	An issue existed in the handling of snapshots. The issue was resolved with improved permissions logic. This issue is fixed in macOS Big Sur 11.0.1. A malicious application may be able to preview files it does not have access to. **CVE ID : CVE-2020-27900**	N/A	O-APP-MACO-171220/564
Improper Privilege Management	08-Dec-20	9.3	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Big Sur 11.0.1. An application may be able to gain elevated privileges. **CVE ID : CVE-2020-27903**	https://support.apple.com/kb/HT212011	O-APP-MACO-171220/565
N/A	08-Dec-20	9.3	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1. An application may be able to execute arbitrary code with kernel	N/A	O-APP-MACO-171220/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. **CVE ID : CVE-2020-27904**		
Integer Overflow or Wraparound	08-Dec-20	9.3	Multiple integer overflows were addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1. A remote attacker may be able to cause unexpected application termination or heap corruption. **CVE ID : CVE-2020-27906**	https://support.apple.com/kb/HT212011	O-APP-MACO-171220/567
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27910**	https://support.apple.com/kb/HT212011	O-APP-MACO-171220/568
Integer Overflow or Wraparound	08-Dec-20	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-27911**	https://support.apple.com/kb/HT212011	O-APP-MACO-171220/569
Out-of-bounds	08-Dec-20	9.3	An out-of-bounds write was addressed with improved input validation. This issue is	https://support.apple.com/kb/HT2	O-APP-MACO-171220/570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-27912**	12011	
Out-of-bounds Write	08-Dec-20	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27916**	https://support.apple.com/kb/HT212011	O-APP-MACO-171220/571
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-27917**	N/A	O-APP-MACO-171220/572
Out-of-bounds Write	08-Dec-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a	N/A	O-APP-MACO-171220/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2020-27927**		
Improper Input Validation	08-Dec-20	6.8	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. Processing a maliciously crafted font may lead to arbitrary code execution. **CVE ID : CVE-2020-27930**	N/A	O-APP-MACO-171220/574
Access of Resource Using Incompatible Type ('Type Confusion')	08-Dec-20	9.3	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to execute arbitrary code with kernel privileges.	N/A	O-APP-MACO-171220/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-27932		
Improper Initialization	08-Dec-20	7.1	A memory initialization issue was addressed. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to disclose kernel memory. **CVE ID : CVE-2020-27950**	N/A	O-APP-MACO-171220/576
Information Exposure	08-Dec-20	4.3	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0. A remote attacker may be able to leak memory. **CVE ID : CVE-2020-9849**	N/A	O-APP-MACO-171220/577
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges.	N/A	O-APP-MACO-171220/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9965		
mac_os					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-20	6.8	A heap overflow vulnerability exists in Pixar OpenUSD 20.05 when the software parses compressed sections in binary USD files. A specially crafted USDC file format path jumps decompression heap overflow in a way path jumps are processed. To trigger this vulnerability, the victim needs to open an attacker-provided malformed file. **CVE ID : CVE-2020-13493**	N/A	O-APP-MAC_-171220/579
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-20	4.3	A heap overflow vulnerability exists in the Pixar OpenUSD 20.05 parsing of compressed string tokens in binary USD files. A specially crafted malformed file can trigger a heap overflow which can result in out of bounds memory access which could lead to information disclosure. This vulnerability could be used to bypass mitigations and aid further exploitation. To trigger this vulnerability, victim needs to access an attacker-provided malformed file. **CVE ID : CVE-2020-13494**	N/A	O-APP-MAC_-171220/580
Out-of-bounds Read	02-Dec-20	4.3	An exploitable vulnerability exists in the way Pixar	N/A	O-APP-MAC_-171220/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OpenUSD 20.05 handles parses certain encoded types. A specially crafted malformed file can trigger an arbitrary out of bounds memory access in TfToken Type Index. This vulnerability could be used to bypass mitigations and aid further exploitation. To trigger this vulnerability, the victim needs to access an attacker-provided malformed file. **CVE ID : CVE-2020-13496**		
Out-of-bounds Read	02-Dec-20	4.3	An exploitable vulnerability exists in the way Pixar OpenUSD 20.05 handles parses certain encoded types. A specially crafted malformed file can trigger an arbitrary out of bounds memory access in String Type Index. This vulnerability could be used to bypass mitigations and aid further exploitation. To trigger this vulnerability, the victim needs to access an attacker-provided malformed file. **CVE ID : CVE-2020-13497**	N/A	O-APP-MAC_-171220/582
Out-of-bounds Read	02-Dec-20	4.3	An exploitable vulnerability exists in the way Pixar OpenUSD 20.05 handles parses certain encoded types. A specially crafted malformed file can trigger an arbitrary out of bounds	N/A	O-APP-MAC_-171220/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory access in SdfPath Type Index. This vulnerability could be used to bypass mitigations and aid further exploitation. To trigger this vulnerability, the victim needs to access an attacker-provided malformed file. **CVE ID : CVE-2020-13498**		
N/A	08-Dec-20	4.3	The issue was addressed with additional user controls. This issue is fixed in macOS Big Sur 11.0.1. Users may be unable to remove metadata indicating where files were downloaded from. **CVE ID : CVE-2020-27894**	N/A	O-APP-MAC_-171220/584
iphone_os					
N/A	08-Dec-20	2.1	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A local user may be able to read arbitrary files. **CVE ID : CVE-2020-10002**	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/585
Improper Link Resolution Before File Access ('Link Following')	08-Dec-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS	N/A	O-APP-IPHO-171220/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			14.2, tvOS 14.2, watchOS 7.1. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-10003**		
N/A	08-Dec-20	6.8	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-10004**	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/587
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-20	4.6	A path handling issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-10010**	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/588
Out-of-bounds Read	08-Dec-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 14.2 and iPadOS 14.2, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-10011**	N/A	O-APP-IPHO-171220/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Dec-20	9.3	A logic issue was addressed with improved state management. This issue is fixed in tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-10013**	N/A	O-APP-IPHO-171220/590
N/A	08-Dec-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-10016**	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/591
Out-of-bounds Write	08-Dec-20	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-10017**	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/592
Improper Authentication	08-Dec-20	2.1	An authentication issue was addressed with improved state management. This issue is fixed in iOS 14.2 and iPadOS 14.2. A person with physical access to an iOS device may be able to access stored passwords without	N/A	O-APP-IPHO-171220/593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication. **CVE ID : CVE-2020-27902**		
N/A	08-Dec-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-27905**	N/A	O-APP-IPHO-171220/594
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27909**	N/A	O-APP-IPHO-171220/595
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27910**	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/596
Integer Overflow or Wraparound	08-Dec-20	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2,	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iTunes 12.11 for Windows. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-27911**		
Out-of-bounds Write	08-Dec-20	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-27912**	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/598
Out-of-bounds Write	08-Dec-20	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27916**	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/599
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may	N/A	O-APP-IPHO-171220/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to code execution. **CVE ID : CVE-2020-27917**		
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, Safari 14.0.1, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-27918**	N/A	O-APP-IPHO-171220/601
N/A	08-Dec-20	1.9	An issue existed in the handling of incoming calls. The issue was addressed with additional state checks. This issue is fixed in iOS 14.2 and iPadOS 14.2. A user may answer two calls simultaneously without indication they have answered a second call. **CVE ID : CVE-2020-27925**	N/A	O-APP-IPHO-171220/602
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 14.2 and iPadOS 14.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-27926**	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/603
Out-of-bounds	08-Dec-20	6.8	An out-of-bounds write issue was addressed with	N/A	O-APP-IPHO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2020-27927**		171220/604
N/A	08-Dec-20	4.3	A logic issue existed in the handling of Group FaceTime calls. The issue was addressed with improved state management. This issue is fixed in iOS 12.4.9. A user may send video in Group FaceTime calls without knowing that they have done so. **CVE ID : CVE-2020-27929**	N/A	O-APP-IPHO-171220/605
Improper Input Validation	08-Dec-20	6.8	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. Processing a maliciously crafted font may lead to arbitrary code execution. **CVE ID : CVE-2020-27930**	N/A	O-APP-IPHO-171220/606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	08-Dec-20	9.3	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-27932**	N/A	O-APP-IPHO-171220/607
Improper Initialization	08-Dec-20	7.1	A memory initialization issue was addressed. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to disclose kernel memory. **CVE ID : CVE-2020-27950**	N/A	O-APP-IPHO-171220/608
Out-of-bounds Read	08-Dec-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			14.0, iOS 14.0 and iPadOS 14.0. A malicious application may be able to read restricted memory. **CVE ID : CVE-2020-9943**		
Out-of-bounds Read	08-Dec-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to read restricted memory. **CVE ID : CVE-2020-9944**	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/610
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, Safari 14.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9947**	N/A	O-APP-IPHO-171220/611
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra, tvOS 14.0. An	N/A	O-APP-IPHO-171220/612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9949**		
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, tvOS 14.0, Safari 14.0, iOS 14.0 and iPadOS 14.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9950**	N/A	O-APP-IPHO-171220/613
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in watchOS 7.0, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave, iOS 14.0 and iPadOS 14.0. Playing a malicious audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9954**	N/A	O-APP-IPHO-171220/614
N/A	08-Dec-20	4.3	The issue was addressed with improved handling of icon caches. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A malicious app may be able to determine the existence of files on the computer. **CVE ID : CVE-2020-9963**	N/A	O-APP-IPHO-171220/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9965**	N/A	O-APP-IPHO-171220/616
Out-of-bounds Read	08-Dec-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9966**	N/A	O-APP-IPHO-171220/617
N/A	08-Dec-20	1.9	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. A local user may be able to view senstive user information. **CVE ID : CVE-2020-9969**	N/A	O-APP-IPHO-171220/618
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 14.0 and iPadOS 14.0. Processing a maliciously crafted USD file may lead to unexpected application termination or	N/A	O-APP-IPHO-171220/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-9972**		
N/A	08-Dec-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9974**	https://support.apple.com/kb/HT212011	O-APP-IPHO-171220/620
Improper Input Validation	08-Dec-20	4.3	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A malicious application may be able to determine a user's open tabs in Safari. **CVE ID : CVE-2020-9977**	N/A	O-APP-IPHO-171220/621
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted file may lead to arbitrary code	N/A	O-APP-IPHO-171220/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-9981**		
N/A	08-Dec-20	2.1	The issue was addressed with improved deletion. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A local user may be able to discover a user's deleted messages. **CVE ID : CVE-2020-9988**	N/A	O-APP-IPHO-171220/623
N/A	08-Dec-20	2.1	The issue was addressed with improved deletion. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0. A local user may be able to discover a user's deleted messages. **CVE ID : CVE-2020-9989**	N/A	O-APP-IPHO-171220/624
N/A	08-Dec-20	5	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iCloud for Windows 7.21, tvOS 14.0. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9991**	N/A	O-APP-IPHO-171220/625
Improper Restriction of Rendered UI Layers or Frames	08-Dec-20	4.3	The issue was addressed with improved UI handling. This issue is fixed in watchOS 7.0, Safari 14.0, iOS 14.0 and iPadOS 14.0. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2020-9993**	N/A	O-APP-IPHO-171220/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A malicious application may be able to elevate privileges. **CVE ID : CVE-2020-9996**	N/A	O-APP-IPHO-171220/627
mac_os_x					
N/A	08-Dec-20	2.1	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A local user may be able to read arbitrary files. **CVE ID : CVE-2020-10002**	https://support.apple.com/kb/HT212011	O-APP-MAC_-171220/628
Improper Link Resolution Before File Access ('Link Following')	08-Dec-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-10003**	N/A	O-APP-MAC_-171220/629
N/A	08-Dec-20	6.8	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2. Opening a maliciously	https://support.apple.com/kb/HT212011	O-APP-MAC_-171220/630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-10004**		
N/A	08-Dec-20	4.3	This issue was addressed with improved entitlements. This issue is fixed in macOS Big Sur 11.0.1. A malicious application may be able to access restricted files. **CVE ID : CVE-2020-10006**	N/A	O-APP-MAC_-171220/631
N/A	08-Dec-20	2.1	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-10007**	https://support.apple.com/kb/HT212011	O-APP-MAC_-171220/632
N/A	08-Dec-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2020-10009**	https://support.apple.com/kb/HT212011	O-APP-MAC_-171220/633
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-20	4.6	A path handling issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A local attacker may be able to elevate their privileges.	https://support.apple.com/kb/HT212011	O-APP-MAC_-171220/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10010		
Out-of-bounds Read	08-Dec-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 14.2 and iPadOS 14.2, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-10011**	N/A	O-APP-MAC_-171220/635
Out-of-bounds Write	08-Dec-20	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-10017**	https://support.apple.com/kb/HT212011	O-APP-MAC_-171220/636
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-20	4.3	A path handling issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.0.1. A remote attacker may be able to modify the file system. **CVE ID : CVE-2020-27896**	https://support.apple.com/kb/HT212011	O-APP-MAC_-171220/637
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS	N/A	O-APP-MAC_-171220/638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			14.2 and iPadOS 14.2, iCloud for Windows 11.5, Safari 14.0.1, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-27918**		
Improper Input Validation	08-Dec-20	6.8	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. Processing a maliciously crafted font may lead to arbitrary code execution. **CVE ID : CVE-2020-27930**	N/A	O-APP-MAC_-171220/639
Access of Resource Using Incompatible Type ('Type Confusion')	08-Dec-20	9.3	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental	N/A	O-APP-MAC_-171220/640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Update, macOS Catalina 10.15.7 Update. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-27932**		
N/A	08-Dec-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra. Processing a maliciously crafted email may lead to writing arbitrary files. **CVE ID : CVE-2020-9922**	N/A	O-APP-MAC_-171220/641
Improper Restriction of Rendered UI Layers or Frames	08-Dec-20	4.3	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, Safari 13.1.2. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2020-9942**	N/A	O-APP-MAC_-171220/642
Out-of-bounds Read	08-Dec-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. A malicious application may be able to read restricted memory. **CVE ID : CVE-2020-9943**	https://support.apple.com/kb/HT212011	O-APP-MAC_-171220/643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Dec-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to read restricted memory. **CVE ID : CVE-2020-9944**	https://support.apple.com/kb/HT212011	O-APP-MAC_-171220/644
Improper Restriction of Rendered UI Layers or Frames	08-Dec-20	4.3	A spoofing issue existed in the handling of URLs. This issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, Safari 14.0.1. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2020-9945**	N/A	O-APP-MAC_-171220/645
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra, tvOS 14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9949**	N/A	O-APP-MAC_-171220/646
Buffer Copy without Checking Size of Input	08-Dec-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in watchOS 7.0, tvOS	N/A	O-APP-MAC_-171220/647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave, iOS 14.0 and iPadOS 14.0. Playing a malicious audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9954**		
N/A	08-Dec-20	4.3	The issue was addressed with improved handling of icon caches. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A malicious app may be able to determine the existence of files on the computer. **CVE ID : CVE-2020-9963**	N/A	O-APP-MAC_-171220/648
Out-of-bounds Read	08-Dec-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9966**	N/A	O-APP-MAC_-171220/649
N/A	08-Dec-20	1.9	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. A local user may be able to view senstive user information.	N/A	O-APP-MAC_-171220/650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9969		
N/A	08-Dec-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9974**	https://support.apple.com/kb/HT212011	O-APP-MAC_-171220/651
Improper Input Validation	08-Dec-20	4.3	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A malicious application may be able to determine a user's open tabs in Safari. **CVE ID : CVE-2020-9977**	N/A	O-APP-MAC_-171220/652
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted file may lead to arbitrary code execution.	N/A	O-APP-MAC_-171220/653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9981		
N/A	08-Dec-20	2.1	The issue was addressed with improved deletion. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A local user may be able to discover a user's deleted messages. **CVE ID : CVE-2020-9988**	N/A	O-APP-MAC_-171220/654
N/A	08-Dec-20	2.1	The issue was addressed with improved deletion. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0. A local user may be able to discover a user's deleted messages. **CVE ID : CVE-2020-9989**	N/A	O-APP-MAC_-171220/655
N/A	08-Dec-20	5	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iCloud for Windows 7.21, tvOS 14.0. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9991**	N/A	O-APP-MAC_-171220/656
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A malicious application may be able to elevate privileges. **CVE ID : CVE-2020-9996**	N/A	O-APP-MAC_-171220/657
Improper	08-Dec-20	6.8	A memory corruption issue	N/A	O-APP-MAC_-

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 macOS Big Sur 11.0.1, iTunes for Windows 12.10.9. Processing a maliciously crafted text file may lead to arbitrary code execution. **CVE ID : CVE-2020-9999**		171220/658
watchos					
N/A	08-Dec-20	2.1	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A local user may be able to read arbitrary files. **CVE ID : CVE-2020-10002**	https://support.apple.com/kb/HT212011	O-APP-WATC-171220/659
Improper Link Resolution Before File Access ('Link Following')	08-Dec-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-10003**	N/A	O-APP-WATC-171220/660
Improper Limitation of a Pathname to a Restricted	08-Dec-20	4.6	A path handling issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS	https://support.apple.com/kb/HT212011	O-APP-WATC-171220/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			14.2, watchOS 7.1. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-10010**		
N/A	08-Dec-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-10016**	https://support.apple.com/kb/HT212011	O-APP-WATC-171220/662
Out-of-bounds Write	08-Dec-20	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-10017**	https://support.apple.com/kb/HT212011	O-APP-WATC-171220/663
N/A	08-Dec-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-27905**	N/A	O-APP-WATC-171220/664
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is	N/A	O-APP-WATC-171220/665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixed in iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27909**		
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27910**	https://support.apple.com/kb/HT212011	O-APP-WATC-171220/666
Integer Overflow or Wraparound	08-Dec-20	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-27911**	https://support.apple.com/kb/HT212011	O-APP-WATC-171220/667
Out-of-bounds Write	08-Dec-20	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing a maliciously	https://support.apple.com/kb/HT212011	O-APP-WATC-171220/668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-27912**		
Out-of-bounds Write	08-Dec-20	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27916**	https://support.apple.com/kb/HT212011	O-APP-WATC-171220/669
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-27917**	N/A	O-APP-WATC-171220/670
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, Safari 14.0.1, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	O-APP-WATC-171220/671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-27918		
Out-of-bounds Write	08-Dec-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2020-27927**	N/A	O-APP-WATC-171220/672
Improper Input Validation	08-Dec-20	6.8	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. Processing a maliciously crafted font may lead to arbitrary code execution. **CVE ID : CVE-2020-27930**	N/A	O-APP-WATC-171220/673
Access of Resource Using Incompatible Type ('Type Confusion')	08-Dec-20	9.3	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2	N/A	O-APP-WATC-171220/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-27932**		
Improper Initialization	08-Dec-20	7.1	A memory initialization issue was addressed. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to disclose kernel memory. **CVE ID : CVE-2020-27950**	N/A	O-APP-WATC-171220/675
Information Exposure	08-Dec-20	4.3	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0. A remote attacker may be able to leak memory. **CVE ID : CVE-2020-9849**	N/A	O-APP-WATC-171220/676
Out-of-	08-Dec-20	4.3	An out-of-bounds read was	https://sup	O-APP-WATC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. A malicious application may be able to read restricted memory. **CVE ID : CVE-2020-9943**	port.apple.com/kb/HT212011	171220/677
Out-of-bounds Read	08-Dec-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to read restricted memory. **CVE ID : CVE-2020-9944**	https://support.apple.com/kb/HT212011	O-APP-WATC-171220/678
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, Safari 14.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9947**	N/A	O-APP-WATC-171220/679
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, macOS	N/A	O-APP-WATC-171220/680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra, tvOS 14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9949**		
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, tvOS 14.0, Safari 14.0, iOS 14.0 and iPadOS 14.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9950**	N/A	O-APP-WATC-171220/681
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in watchOS 7.0, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave, iOS 14.0 and iPadOS 14.0. Playing a malicious audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9954**	N/A	O-APP-WATC-171220/682
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS	N/A	O-APP-WATC-171220/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9965**		
Out-of-bounds Read	08-Dec-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9966**	N/A	O-APP-WATC-171220/684
N/A	08-Dec-20	1.9	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. A local user may be able to view senstive user information. **CVE ID : CVE-2020-9969**	N/A	O-APP-WATC-171220/685
N/A	08-Dec-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9974**	https://support.apple.com/kb/HT212011	O-APP-WATC-171220/686
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0,	N/A	O-APP-WATC-171220/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2020-9981**		
N/A	08-Dec-20	2.1	The issue was addressed with improved deletion. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0. A local user may be able to discover a user's deleted messages. **CVE ID : CVE-2020-9989**	N/A	O-APP-WATC-171220/688
N/A	08-Dec-20	5	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iCloud for Windows 7.21, tvOS 14.0. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9991**	N/A	O-APP-WATC-171220/689
Improper Restriction of Rendered UI Layers or Frames	08-Dec-20	4.3	The issue was addressed with improved UI handling. This issue is fixed in watchOS 7.0, Safari 14.0, iOS 14.0 and iPadOS 14.0. Visiting a malicious website may lead to address bar spoofing.	N/A	O-APP-WATC-171220/690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9993		
tvos					
N/A	08-Dec-20	2.1	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A local user may be able to read arbitrary files. **CVE ID : CVE-2020-10002**	https://support.apple.com/kb/HT212011	O-APP-TVOS-171220/691
Improper Link Resolution Before File Access ('Link Following')	08-Dec-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-10003**	N/A	O-APP-TVOS-171220/692
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-20	4.6	A path handling issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-10010**	https://support.apple.com/kb/HT212011	O-APP-TVOS-171220/693
N/A	08-Dec-20	9.3	A logic issue was addressed with improved state management. This issue is fixed in tvOS 14.0, iOS 14.0 and iPadOS 14.0. An	N/A	O-APP-TVOS-171220/694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-10013**		
N/A	08-Dec-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-10016**	https://support.apple.com/kb/HT212011	O-APP-TVOS-171220/695
Out-of-bounds Write	08-Dec-20	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-10017**	https://support.apple.com/kb/HT212011	O-APP-TVOS-171220/696
N/A	08-Dec-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-27905**	N/A	O-APP-TVOS-171220/697
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is	N/A	O-APP-TVOS-171220/698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixed in iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27909**		
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27910**	https://support.apple.com/kb/HT212011	O-APP-TVOS-171220/699
Integer Overflow or Wraparound	08-Dec-20	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-27911**	https://support.apple.com/kb/HT212011	O-APP-TVOS-171220/700
Out-of-bounds Write	08-Dec-20	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing a maliciously	https://support.apple.com/kb/HT212011	O-APP-TVOS-171220/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-27912**		
Out-of-bounds Write	08-Dec-20	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27916**	https://support.apple.com/kb/HT212011	O-APP-TVOS-171220/702
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-27917**	N/A	O-APP-TVOS-171220/703
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, Safari 14.0.1, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	O-APP-TVOS-171220/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-27918		
Out-of-bounds Write	08-Dec-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2020-27927**	N/A	O-APP-TVOS-171220/705
Information Exposure	08-Dec-20	4.3	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0. A remote attacker may be able to leak memory. **CVE ID : CVE-2020-9849**	N/A	O-APP-TVOS-171220/706
Out-of-bounds Read	08-Dec-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. A malicious application may be able to read restricted memory. **CVE ID : CVE-2020-9943**	https://support.apple.com/kb/HT212011	O-APP-TVOS-171220/707
Out-of-bounds Read	08-Dec-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur	https://support.apple.com/kb/HT212011	O-APP-TVOS-171220/708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to read restricted memory. **CVE ID : CVE-2020-9944**		
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, Safari 14.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9947**	N/A	O-APP-TVOS-171220/709
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra, tvOS 14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9949**	N/A	O-APP-TVOS-171220/710
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, tvOS 14.0, Safari 14.0, iOS	N/A	O-APP-TVOS-171220/711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			14.0 and iPadOS 14.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9950**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in watchOS 7.0, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave, iOS 14.0 and iPadOS 14.0. Playing a malicious audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9954**	N/A	O-APP-TVOS-171220/712
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9965**	N/A	O-APP-TVOS-171220/713
Out-of-bounds Read	08-Dec-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges.	N/A	O-APP-TVOS-171220/714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9966		
N/A	08-Dec-20	1.9	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. A local user may be able to view senstive user information. **CVE ID : CVE-2020-9969**	N/A	O-APP-TVOS-171220/715
N/A	08-Dec-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9974**	https://support.apple.com/kb/HT212011	O-APP-TVOS-171220/716
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2020-9981**	N/A	O-APP-TVOS-171220/717
N/A	08-Dec-20	5	This issue was addressed	N/A	O-APP-TVOS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with improved checks. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iCloud for Windows 7.21, tvOS 14.0. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9991**		171220/718
ipados					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-20	4.6	A path handling issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-10010**	https://support.apple.com/kb/HT212011	O-APP-IPAD-171220/719
Out-of-bounds Read	08-Dec-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 14.2 and iPadOS 14.2, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-10011**	N/A	O-APP-IPAD-171220/720
N/A	08-Dec-20	9.3	A logic issue was addressed with improved state management. This issue is fixed in tvOS 14.0, iOS 14.0 and iPadOS 14.0. An	N/A	O-APP-IPAD-171220/721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-10013**		
N/A	08-Dec-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-10016**	https://support.apple.com/kb/HT212011	O-APP-IPAD-171220/722
Improper Authentication	08-Dec-20	2.1	An authentication issue was addressed with improved state management. This issue is fixed in iOS 14.2 and iPadOS 14.2. A person with physical access to an iOS device may be able to access stored passwords without authentication. **CVE ID : CVE-2020-27902**	N/A	O-APP-IPAD-171220/723
N/A	08-Dec-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-27905**	N/A	O-APP-IPAD-171220/724
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is	N/A	O-APP-IPAD-171220/725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixed in iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27909**		
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27910**	https://support.apple.com/kb/HT212011	O-APP-IPAD-171220/726
Integer Overflow or Wraparound	08-Dec-20	9.3	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-27911**	https://support.apple.com/kb/HT212011	O-APP-IPAD-171220/727
Out-of-bounds Write	08-Dec-20	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing a maliciously	https://support.apple.com/kb/HT212011	O-APP-IPAD-171220/728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-27912**		
Out-of-bounds Write	08-Dec-20	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-27916**	https://support.apple.com/kb/HT212011	O-APP-IPAD-171220/729
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-27917**	N/A	O-APP-IPAD-171220/730
N/A	08-Dec-20	1.9	An issue existed in the handling of incoming calls. The issue was addressed with additional state checks. This issue is fixed in iOS 14.2 and iPadOS 14.2. A user may answer two calls simultaneously without indication they have answered a second call. **CVE ID : CVE-2020-27925**	N/A	O-APP-IPAD-171220/731
Use After	08-Dec-20	9.3	A use after free issue was addressed with improved	https://support.apple.c	O-APP-IPAD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			memory management. This issue is fixed in iOS 14.2 and iPadOS 14.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-27926**	om/kb/HT212011	171220/732
Out-of-bounds Write	08-Dec-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2020-27927**	N/A	O-APP-IPAD-171220/733
Improper Input Validation	08-Dec-20	6.8	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. Processing a maliciously crafted font may lead to arbitrary code execution. **CVE ID : CVE-2020-27930**	N/A	O-APP-IPAD-171220/734
Access of Resource	08-Dec-20	9.3	A type confusion issue was addressed with improved	N/A	O-APP-IPAD-171220/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Using Incompatible Type ('Type Confusion')			state handling. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-27932**		
Improper Initialization	08-Dec-20	7.1	A memory initialization issue was addressed. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to disclose kernel memory. **CVE ID : CVE-2020-27950**	N/A	O-APP-IPAD-171220/736
Information Exposure	08-Dec-20	4.3	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for	N/A	O-APP-IPAD-171220/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0. A remote attacker may be able to leak memory. **CVE ID : CVE-2020-9849**		
Out-of-bounds Read	08-Dec-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. A malicious application may be able to read restricted memory. **CVE ID : CVE-2020-9943**	https://support.apple.com/kb/HT212011	O-APP-IPAD-171220/738
Out-of-bounds Read	08-Dec-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to read restricted memory. **CVE ID : CVE-2020-9944**	https://support.apple.com/kb/HT212011	O-APP-IPAD-171220/739
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, Safari 14.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9947**	N/A	O-APP-IPAD-171220/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra, tvOS 14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9949**	N/A	O-APP-IPAD-171220/741
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, tvOS 14.0, Safari 14.0, iOS 14.0 and iPadOS 14.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9950**	N/A	O-APP-IPAD-171220/742
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in watchOS 7.0, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave, iOS 14.0 and iPadOS 14.0. Playing a malicious audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9954**	N/A	O-APP-IPAD-171220/743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Dec-20	4.3	The issue was addressed with improved handling of icon caches. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A malicious app may be able to determine the existence of files on the computer. **CVE ID : CVE-2020-9963**	N/A	O-APP-IPAD-171220/744
Out-of-bounds Read	08-Dec-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9965**	N/A	O-APP-IPAD-171220/745
ipad_os					
N/A	08-Dec-20	2.1	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A local user may be able to read arbitrary files. **CVE ID : CVE-2020-10002**	https://support.apple.com/kb/HT212011	O-APP-IPAD-171220/746
Improper Link Resolution Before File Access ('Link Following')	08-Dec-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in macOS Big Sur	N/A	O-APP-IPAD-171220/747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-10003**		
N/A	08-Dec-20	6.8	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-10004**	https://support.apple.com/kb/HT212011	O-APP-IPAD-171220/748
Out-of-bounds Write	08-Dec-20	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-10017**	https://support.apple.com/kb/HT212011	O-APP-IPAD-171220/749
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, Safari 14.0.1, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to arbitrary code	N/A	O-APP-IPAD-171220/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-27918**		
Out-of-bounds Read	08-Dec-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9966**	N/A	O-APP-IPAD-171220/751
N/A	08-Dec-20	1.9	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. A local user may be able to view senstive user information. **CVE ID : CVE-2020-9969**	N/A	O-APP-IPAD-171220/752
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 14.0 and iPadOS 14.0. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9972**	N/A	O-APP-IPAD-171220/753
N/A	08-Dec-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1.	https://support.apple.com/kb/HT212011	O-APP-IPAD-171220/754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9974**		
Improper Input Validation	08-Dec-20	4.3	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A malicious application may be able to determine a user's open tabs in Safari. **CVE ID : CVE-2020-9977**	N/A	O-APP-IPAD-171220/755
Use After Free	08-Dec-20	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2020-9981**	N/A	O-APP-IPAD-171220/756
N/A	08-Dec-20	2.1	The issue was addressed with improved deletion. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A local user may be able to discover a	N/A	O-APP-IPAD-171220/757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user's deleted messages. **CVE ID : CVE-2020-9988**		
N/A	08-Dec-20	2.1	The issue was addressed with improved deletion. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0. A local user may be able to discover a user's deleted messages. **CVE ID : CVE-2020-9989**	N/A	O-APP-IPAD-171220/758
N/A	08-Dec-20	5	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iCloud for Windows 7.21, tvOS 14.0. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9991**	N/A	O-APP-IPAD-171220/759
Improper Restriction of Rendered UI Layers or Frames	08-Dec-20	4.3	The issue was addressed with improved UI handling. This issue is fixed in watchOS 7.0, Safari 14.0, iOS 14.0 and iPadOS 14.0. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2020-9993**	N/A	O-APP-IPAD-171220/760
Use After Free	08-Dec-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A malicious application may be able to elevate privileges.	N/A	O-APP-IPAD-171220/761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9996		
Arubanetworks					
arubaos					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	O-ARU-ARUB-171220/762
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	O-ARU-ARUB-171220/763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**		
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	O-ARU-ARUB-171220/764
sd-wan					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04	O-ARU-SD-W-171220/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**	072en_us	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	O-ARU-SD-W-171220/766
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_U	O-ARU-SD-W-171220/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**	S&docId=emr_na-hpesbnw04072en_us	
askey					
ap5100w_firmware					
Use of Insufficiently Random Values	11-Dec-20	4.3	Askey AP5100W devices through AP5100W_Dual_SIG_1.01.097 are affected by WPS PIN offline brute-force cracking. This arises because of issues with the random number selection for the Diffie-Hellman exchange. By capturing an attempted (and even failed) WPS authentication attempt, it is possible to brute force the overall authentication exchange. This allows an attacker to obtain the recovered WPS PIN in minutes or even seconds, and eventually obtain the Wi-Fi PSK key, gaining	https://www.askey.com.tw/incident_report_notifications.html	O-ASK-AP51-171220/768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the Wi=Fi network. **CVE ID : CVE-2020-15023**		
N/A	11-Dec-20	10	Network Analysis functionality in Askey AP5100W_Dual_SIG_1.01.097 and all prior versions allows remote attackers to execute arbitrary commands via a shell metacharacter in the ping, traceroute, or route options. **CVE ID : CVE-2020-15357**	N/A	O-ASK-AP51-171220/769
Asus					
rt-ac88u_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-Dec-20	5	An injection vulnerability exists in RT-AC88U Download Master before 3.1.0.108. Accessing Main_Login.asp?flag=1&productname=FOOBAR&url=/downloadmaster/task.asp will redirect to the login site, which will show the value of the parameter productname within the title. An attacker might be able to influence the appearance of the login page, aka text injection. **CVE ID : CVE-2020-29655**	N/A	O-ASU-RT-A-171220/770
Information Exposure	09-Dec-20	5	An information disclosure vulnerability exists in RT-AC88U Download Master before 3.1.0.108. A direct access to /downloadmaster/dm_apply.cgi?action_mode=initial&download_type=General&special_cgi=get_language makes it	N/A	O-ASU-RT-A-171220/771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			possible to reach "unknown functionality" in a "known to be easy" manner via an unspecified "public exploit." **CVE ID : CVE-2020-29656**		
atx					
minicmts200a_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Dec-20	5	A Directory Traversal vulnerability exists in ATX miniCMTS200a Broadband Gateway through 2.0 and Pico CMTS through 2.0. Successful exploitation of this vulnerability would allow an unauthenticated attacker to retrieve administrator credentials by sending a malicious POST request. **CVE ID : CVE-2020-28993**	N/A	O-ATX-MINI-171220/772
Canonical					
ubuntu_linux					
Uncontrolled Search Path Element	04-Dec-20	4.4	In some conditions, a snap package built by snapcraft includes the current directory in LD_LIBRARY_PATH, allowing a malicious snap to gain code execution within the context of another snap if both plug the home interface or similar. This issue affects snapcraft versions prior to 4.4.4, prior to 2.43.1+16.04.1, and prior to 2.43.1+18.04.1. **CVE ID : CVE-2020-27348**	N/A	O-CAN-UBUN-171220/773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-Dec-20	2.1	Aptdaemon performed policykit checks after interacting with potentially untrusted files with elevated privileges. This affected versions prior to 1.1.1+bzr982-0ubuntu34.1, 1.1.1+bzr982-0ubuntu32.3, 1.1.1+bzr982-0ubuntu19.5, 1.1.1+bzr982-0ubuntu14.5. **CVE ID : CVE-2020-27349**	N/A	O-CAN-UBUN-171220/774
Integer Overflow or Wraparound	10-Dec-20	4.6	APT had several integer overflows and underflows while parsing .deb packages, aka GHSL-2020-168 GHSL-2020-169, in files apt-pkg/contrib/extracttar.cc, apt-pkg/deb/debfile.cc, and apt-pkg/contrib/arfile.cc. This issue affects: apt 1.2.32ubuntu0 versions prior to 1.2.32ubuntu0.2; 1.6.12ubuntu0 versions prior to 1.6.12ubuntu0.2; 2.0.2ubuntu0 versions prior to 2.0.2ubuntu0.2; 2.1.10ubuntu0 versions prior to 2.1.10ubuntu0.1; **CVE ID : CVE-2020-27350**	https://bugs.launchpad.net/bugs/1899193	O-CAN-UBUN-171220/775
Missing Release of Resource after Effective Lifetime	10-Dec-20	2.1	Various memory and file descriptor leaks were found in apt-python files python/arfile.cc, python/tag.cc, python/tarfile.cc, aka GHSL-2020-170. This issue affects: python-apt 1.1.0~beta1 versions prior to 1.1.0~beta1ubuntu0.16.04.1	https://bugs.launchpad.net/bugs/1899193	O-CAN-UBUN-171220/776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0; 1.6.5ubuntu0 versions prior to 1.6.5ubuntu0.4; 2.0.0ubuntu0 versions prior to 2.0.0ubuntu0.20.04.2; 2.1.3ubuntu1 versions prior to 2.1.3ubuntu1.1; **CVE ID : CVE-2020-27351**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Dec-20	2.1	An Ubuntu-specific patch in PulseAudio created a race condition where the snap policy module would fail to identify a client connection from a snap as coming from a snap if SCM_CREDENTIALS were missing, allowing the snap to connect to PulseAudio without proper confinement. This could be exploited by an attacker to expose sensitive information. Fixed in 1:13.99.3-1ubuntu2, 1:13.99.2-1ubuntu2.1, 1:13.99.1-1ubuntu3.8, 1:11.1-1ubuntu7.11, and 1:8.0-0ubuntu3.15. **CVE ID : CVE-2020-16123**	N/A	O-CAN-UBUN-171220/777
Information Exposure Through an Error Message	09-Dec-20	2.1	The aptdaemon DBus interface disclosed file existence disclosure by setting Terminal/DebconfSocket properties, aka GHSL-2020-192 and GHSL-2020-196. This affected versions prior to 1.1.1+bzr982-0ubuntu34.1, 1.1.1+bzr982-0ubuntu32.3, 1.1.1+bzr982-0ubuntu19.5, 1.1.1+bzr982-	N/A	O-CAN-UBUN-171220/778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0ubuntu14.5. **CVE ID : CVE-2020-16128**		
Contiki-os					
contiki-os					
Out-of-bounds Write	11-Dec-20	7.5	An issue was discovered in the IPv6 stack in Contiki through 3.0. There is an insufficient check for the IPv6 header length. This leads to Denial-of-Service and potential Remote Code Execution via a crafted ICMPv6 echo packet. **CVE ID : CVE-2020-25111**	N/A	O-CON-CONT-171220/779
Out-of-bounds Write	11-Dec-20	7.5	An issue was discovered in the IPv6 stack in Contiki through 3.0. There are inconsistent checks for IPv6 header extension lengths. This leads to Denial-of-Service and potential Remote Code Execution via a crafted ICMPv6 echo packet. **CVE ID : CVE-2020-25112**	N/A	O-CON-CONT-171220/780
contiki					
Loop with Unreachable Exit Condition ('Infinite Loop')	11-Dec-20	5	An issue was discovered in Contiki through 3.0. An infinite loop exists in the uIP TCP/IP stack component when processing IPv6 extension headers in ext_hdr_options_process in net/ipv6/uip6.c. **CVE ID : CVE-2020-13984**	N/A	O-CON-CONT-171220/781
Debian					
debian_linux					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	08-Dec-20	5	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2154ab83e14ede338d2ede9bbe5cdfce5d5a6c9e, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=f960d81215ebf3f65e03d4d5d857fb9b666d6920, https://www.openssl.org/news/secadv/20201208.txt	O-DEB-DEBI-171220/782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w). **CVE ID : CVE-2020-1971**		
Integer Overflow or	10-Dec-20	4.6	APT had several integer overflows and underflows	https://bugs.launchpad	O-DEB-DEBI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			while parsing .deb packages, aka GHSL-2020-168 GHSL-2020-169, in files apt-pkg/contrib/extracttar.cc, apt-pkg/deb/debfile.cc, and apt-pkg/contrib/arfile.cc. This issue affects: apt 1.2.32ubuntu0 versions prior to 1.2.32ubuntu0.2; 1.6.12ubuntu0 versions prior to 1.6.12ubuntu0.2; 2.0.2ubuntu0 versions prior to 2.0.2ubuntu0.2; 2.1.10ubuntu0 versions prior to 2.1.10ubuntu0.1; **CVE ID : CVE-2020-27350**	.net/bugs/1899193	171220/783
Missing Release of Resource after Effective Lifetime	10-Dec-20	2.1	Various memory and file descriptor leaks were found in apt-python files python/arfile.cc, python/tag.cc, python/tarfile.cc, aka GHSL-2020-170. This issue affects: python-apt 1.1.0~beta1 versions prior to 1.1.0~beta1ubuntu0.16.04.10; 1.6.5ubuntu0 versions prior to 1.6.5ubuntu0.4; 2.0.0ubuntu0 versions prior to 2.0.0ubuntu0.20.04.2; 2.1.3ubuntu1 versions prior to 2.1.3ubuntu1.1; **CVE ID : CVE-2020-27351**	https://bugs.launchpad.net/bugs/1899193	O-DEB-DEBI-171220/784
Edimax					
ic-3116w_firmware					
Out-of-bounds Write	01-Dec-20	7.5	A stack-based buffer-overflow exists in Edimax IP-Camera IC-3116W (v3.06)	https://www.edimax.com/edimax	O-EDI-IC-3-171220/785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and IC-3140W (v3.07), which allows an unauthenticated, unauthorized attacker to perform remote-code-execution due to a crafted GET-Request. The overflow occurs in binary ipcam_cgi due to a missing type check in function doGetSysteminfo(). This has been fixed in version: IC-3116W v3.08. **CVE ID : CVE-2020-26762**	/download/download/data/edimax/de/download/for_home/home_network_cameras/home_network_cameras_indoor_fixed/ic-3116w	
ic-3140w_firmware					
Out-of-bounds Write	01-Dec-20	7.5	A stack-based buffer-overflow exists in Edimax IP-Camera IC-3116W (v3.06) and IC-3140W (v3.07), which allows an unauthenticated, unauthorized attacker to perform remote-code-execution due to a crafted GET-Request. The overflow occurs in binary ipcam_cgi due to a missing type check in function doGetSysteminfo(). This has been fixed in version: IC-3116W v3.08. **CVE ID : CVE-2020-26762**	https://www.edimax.com/edimax/download/download/data/edimax/de/download/for_home/home_network_cameras/home_network_cameras_indoor_fixed/ic-3116w	O-EDI-IC-3-171220/786
ethernut					
nut\/os					
Out-of-bounds Read	11-Dec-20	7.5	An issue was discovered in the DNS implementation in Ethernut in Nut/OS 5.1. There is no check on	N/A	O-ETH-NUT\-171220/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			whether a domain name has '\0' termination. This may lead to successful Denial-of-Service, and possibly Remote Code Execution. **CVE ID : CVE-2020-25107**		
Out-of-bounds Write	11-Dec-20	7.5	An issue was discovered in the DNS implementation in Ethernut in Nut/OS 5.1. The DNS response data length is not checked (it can be set to an arbitrary value from a packet). This may lead to successful Denial-of-Service, and possibly Remote Code Execution. **CVE ID : CVE-2020-25108**	N/A	O-ETH-NUT\-171220/788
Out-of-bounds Read	11-Dec-20	7.5	An issue was discovered in the DNS implementation in Ethernut in Nut/OS 5.1. The number of DNS queries/responses (set in a DNS header) is not checked against the data present. This may lead to successful Denial-of-Service, and possibly Remote Code Execution. **CVE ID : CVE-2020-25109**	N/A	O-ETH-NUT\-171220/789
Out-of-bounds Read	11-Dec-20	7.5	An issue was discovered in the DNS implementation in Ethernut in Nut/OS 5.1. The length byte of a domain name in a DNS query/response is not checked, and is used for internal memory operations. This may lead to successful	N/A	O-ETH-NUT\-171220/790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial-of-Service, and possibly Remote Code Execution. **CVE ID : CVE-2020-25110**		
Fedoraproject					
fedora					
Use After Free	03-Dec-20	6.8	An exploitable use-after-free vulnerability exists in WebKitGTK browser version 2.30.1 x64. A specially crafted HTML web page can cause a use-after-free condition, resulting in a remote code execution. The victim needs to visit a malicious web site to trigger this vulnerability. **CVE ID : CVE-2020-13584**	N/A	O-FED-FEDO-171220/791
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-20	4.3	A flaw was found in the check_chunk_name() function of pngcheck-2.4.0. An attacker able to pass a malicious file to be processed by pngcheck could cause a temporary denial of service, posing a low risk to application availability. **CVE ID : CVE-2020-27818**	https://bugzilla.redhat.com/show_bug.cgi?id=1902011	O-FED-FEDO-171220/792
Google					
android					
N/A	09-Dec-20	4	If the Remote Debugging via USB feature was enabled in Firefox for Android on an Android version prior to Android 6.0, untrusted apps could have connected to the	https://www.mozilla.org/security/advisories/mfsa2020-50/	O-GOO-ANDR-171220/793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			feature and operated with the privileges of the browser to read and interact with web content. The feature was implemented as a unix domain socket, protected by the Android SELinux policy; however, SELinux was not enforced for versions prior to 6.0. This was fixed by removing the Remote Debugging via USB feature from affected devices. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83. **CVE ID : CVE-2020-26964**		
Huawei					
honor_20_pro_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro,	N/A	O-HUA-HONO-171220/794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
yale-l61a_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	O-HUA-YALE-171220/795
hima-l29c_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user	N/A	O-HUA-HIMA-171220/796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
sydneym-al00_firmware					
Out-of-bounds Write	01-Dec-20	4.6	HUAWEI nova 4 versions earlier than 10.0.0.165(C01E34R2P4) and SydneyM-AL00 versions earlier than 10.0.0.165(C00E66R1P5) have an out-of-bounds read and write vulnerability. An attacker with specific permissions crafts malformed packet with specific parameter and sends the packet to the affected products. Due to insufficient validation of packet, which may be exploited to cause the information leakage or arbitrary code execution. **CVE ID : CVE-2020-9117**	N/A	O-HUA-SYDN-171220/797
yale-tl00b_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	O-HUA-YALE-171220/798
yalep-al10b_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product	N/A	O-HUA-YALE-171220/799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
laya-al00ep_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	O-HUA-LAYA-171220/800
princeton-al10b_firmware					
Buffer Copy without Checking Size of Input ('Classic	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain	N/A	O-HUA-PRIN-171220/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
tony-al00b_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-	N/A	O-HUA-TONY-171220/802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
mate_20_pro_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	O-HUA-MATE-171220/803
nova_4_firmware					
Out-of-bounds Write	01-Dec-20	4.6	HUAWEI nova 4 versions earlier than 10.0.0.165(C01E34R2P4) and SydneyM-AL00 versions earlier than 10.0.0.165(C00E66R1P5) have an out-of-bounds read and write vulnerability. An attacker with specific permissions crafts	N/A	O-HUA-NOVA-171220/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malformed packet with specific parameter and sends the packet to the affected products. Due to insufficient validation of packet, which may be exploited to cause the information leakage or arbitrary code execution. **CVE ID : CVE-2020-9117**		
p30_pro_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	O-HUA-P30_-171220/805
p30_firmware					
Buffer Copy without Checking	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The	N/A	O-HUA-P30_-171220/806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
mate_20_x_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro,	N/A	O-HUA-MATE-171220/807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
mate_20_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	O-HUA-MATE-171220/808
IBM					
AIX					
Improper Privilege Management	10-Dec-20	7.2	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a local user to exploit a vulnerability in the ksu user command to gain root privileges. IBM X-Force ID: 189960.	https://www.ibm.com/support/pages/node/6380430	O-IBM-AIX-171220/809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4829		
vios					
Improper Privilege Management	10-Dec-20	7.2	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a local user to exploit a vulnerability in the ksu user command to gain root privileges. IBM X-Force ID: 189960. **CVE ID : CVE-2020-4829**	https://www.ibm.com/support/pages/node/6380430	O-IBM-VIOS-171220/810
inspur					
ns5488m5_firmware					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	O-INS-NS54-171220/811
ns5484m5_firmware					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard	https://en.inspur.com/en/security_bulletins/security_advi	O-INS-NS54-171220/812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	sory2/2543921/index.html	
ns5482m5_firmware					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	O-INS-NS54-171220/813
nf5280m5_firmware					
Improper	07-Dec-20	6.5	Inspur NF5266M5 through	https://en.i	O-INS-NF52-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Verification of Cryptographic Signature			3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	nspur.com/en/security_bulletins/security_advisory2/2543921/index.html	171220/814
nf5468m5_firmware					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC.	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	O-INS-NF54-171220/815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-26122		
nf5488m5-d_firmware					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	O-INS-NF54-171220/816
nf5180m5_firmware					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	O-INS-NF51-171220/817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**		
nf5270m5_firmware					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	O-INS-NF52-171220/818
nf5260m5_firmware					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	O-INS-NF52-171220/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**		
nf5266m5_firmware					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	O-INS-NF52-171220/820
nf5466m5_firmware					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	O-INS-NF54-171220/821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**		
nf5486m5_firmware					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	O-INS-NF54-171220/822
nf8480m5_firmware					
Improper Verification of Cryptographi	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator	https://en.inspur.com/en/security_bulletins/s	O-INS-NF84-171220/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c Signature			privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	ecurity_advisory2/2543921/index.html	
nf8260m5_firmware					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	O-INS-NF82-171220/824
ns5162m5_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	O-INS-NS51-171220/825
kia					
head_unit_firmware					
Incorrect Default Permissions	01-Dec-20	4.6	Kia Motors Head Unit with Software version: SOP.003.30.18.0703, SOP.005.7.181019, and SOP.007.1.191209 may allow an attacker to inject unauthorized commands, by executing the micomd executable deamon, to trigger unintended functionalities. In addition, this executable may be used by an attacker to inject commands to generate CAN frames that are sent into the M-CAN bus (Multimedia CAN bus) of the vehicle.	N/A	O-KIA-HEAD-171220/826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8539		
Linux					
linux_kernel					
Out-of-bounds Write	02-Dec-20	8.3	An out-of-bounds memory write flaw was found in how the Linux kernel's Voice Over IP H.323 connection tracking functionality handled connections on ipv6 port 1720. This flaw allows an unauthenticated remote user to crash the system, causing a denial of service. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2020-14305**	https://security.netapp.com/advisory/ntap-20201210-0004/	O-LIN-LINU-171220/827
Use After Free	03-Dec-20	4.6	A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker with permission to monitor perf events to corrupt memory and possibly escalate privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2020-14351**	N/A	O-LIN-LINU-171220/828
Use After Free	03-Dec-20	4.6	A flaw was found in the Linux kernel's futex implementation. This flaw allows a local attacker to corrupt system memory or	N/A	O-LIN-LINU-171220/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges when creating a futex on a filesystem that is about to be unmounted. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2020-14381**		
Use After Free	02-Dec-20	1.9	A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctls KDGKBSENT and KDSKBSENT. A local user could use this flaw to get read memory access out of bounds. The highest threat from this vulnerability is to data confidentiality. **CVE ID : CVE-2020-25656**	N/A	O-LIN-LINU-171220/830
Uncontrolled Resource Consumption	02-Dec-20	4.9	A flaw memory leak in the Linux kernel performance monitoring subsystem was found in the way if using PERF_EVENT_IOC_SET_FILTER. A local user could use this flaw to starve the resources causing denial of service. **CVE ID : CVE-2020-25704**	N/A	O-LIN-LINU-171220/831
Use After Free	11-Dec-20	7.2	A flaw was found in the Linux kernels implementation of MIDI (kernel 5.7-rc6), where an attacker with a local account and the permissions to issue an ioctl commands to midi	N/A	O-LIN-LINU-171220/832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices, could trigger a use-after-free. A write to this specific memory while freed and before use could cause the flow of execution to change and possibly allow for memory corruption or privilege escalation. **CVE ID : CVE-2020-27786**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Dec-20	5.4	A use-after-free flaw was found in kernel/trace/ring_buffer.c in Linux kernel (before 5.10-rc1). There was a race problem in trace_open and resize of cpu buffer running parallely on different cpus, may cause a denial of service problem (DOS). This flaw could even allow a local attacker with special user privilege to a kernel information leak threat. **CVE ID : CVE-2020-27825**	N/A	O-LIN-LINU-171220/833
N/A	03-Dec-20	7.2	An issue was discovered in the Linux kernel before 5.9.3. io_uring takes a non-refcounted reference to the files_struct of the process that submitted a request, causing execve() to incorrectly optimize unshare_fd(), aka CID-0f2122045b94. **CVE ID : CVE-2020-29534**	N/A	O-LIN-LINU-171220/834
Improper Locking	09-Dec-20	7.2	A locking inconsistency issue was discovered in the tty subsystem of the Linux	N/A	O-LIN-LINU-171220/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel through 5.9.13. drivers/tty/tty_io.c and drivers/tty/tty_jobctrl.c may allow a read-after-free attack against TIOCGSID, aka CID-c8bcd9c5be24. **CVE ID : CVE-2020-29660**		
Improper Locking	09-Dec-20	7.2	A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b. **CVE ID : CVE-2020-29661**	N/A	O-LIN-LINU-171220/836
Microsoft					
windows					
Improper Control of Generation of Code ('Code Injection')	10-Dec-20	6.5	The member center function in fastadmin V1.0.0.20200506_beta is vulnerable to a Server-Side Template Injection (SSTI) vulnerability. **CVE ID : CVE-2020-25967**	N/A	O-MIC-WIND-171220/837
Uncontrolled Search Path Element	11-Dec-20	3.7	Adobe Prelude version 9.0.1 (and earlier) is affected by an uncontrolled search path element that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2020-24440**	https://helpx.adobe.com/security/products/prelude/apsb20-70.html	O-MIC-WIND-171220/838
Uncontrolled	11-Dec-20	3.7	Adobe Lightroom Classic	https://hel	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Search Path Element			version 10.0 (and earlier) for Windows is affected by an uncontrolled search path vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2020-24447**	px.adobe.com/security/products/lightroom/apsb20-74.html	171220/839
N/A	09-Dec-20	4.3	Searching for a single word from the address bar caused an mDNS request to be sent on the local network searching for a hostname consisting of that string; resulting in an information leak. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. **CVE ID : CVE-2020-26966**	https://www.mozilla.org/security/advisories/mfsa2020-50/, https://www.mozilla.org/security/advisories/mfsa2020-51/, https://www.mozilla.org/security/advisories/mfsa2020-52/	O-MIC-WIND-171220/840
windows_10					
Out-of-bounds Write	10-Dec-20	5.1	, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-17131**	N/A	O-MIC-WIND-171220/841
Improper Privilege Management	10-Dec-20	4.6	, aka 'Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-171220/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2020-17103, CVE-2020-17136. **CVE ID : CVE-2020-17134**		
Improper Privilege Management	10-Dec-20	4.6	, aka 'Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-17103, CVE-2020-17134. **CVE ID : CVE-2020-17136**	N/A	O-MIC-WIND-171220/843
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16958**	N/A	O-MIC-WIND-171220/844
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16959**	N/A	O-MIC-WIND-171220/845
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964.	N/A	O-MIC-WIND-171220/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16960		
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16961**	N/A	O-MIC-WIND-171220/847
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16962**	N/A	O-MIC-WIND-171220/848
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16964. **CVE ID : CVE-2020-16963**	N/A	O-MIC-WIND-171220/849
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963. **CVE ID : CVE-2020-16964**	N/A	O-MIC-WIND-171220/850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17092**	N/A	O-MIC-WIND-171220/851
N/A	10-Dec-20	2.1	, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-17138. **CVE ID : CVE-2020-17094**	N/A	O-MIC-WIND-171220/852
N/A	10-Dec-20	9	, aka 'Hyper-V Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17095**	N/A	O-MIC-WIND-171220/853
N/A	10-Dec-20	9	, aka 'Windows NTFS Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17096**	N/A	O-MIC-WIND-171220/854
Improper Privilege Management	10-Dec-20	4.6	, aka 'Windows Digital Media Receiver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17097**	N/A	O-MIC-WIND-171220/855
N/A	10-Dec-20	2.1	, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17098**	N/A	O-MIC-WIND-171220/856
N/A	10-Dec-20	4.6	, aka 'Windows Lock Screen Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-17099**	N/A	O-MIC-WIND-171220/857
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-17134, CVE-2020-17136.	N/A	O-MIC-WIND-171220/858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-17103		
Improper Privilege Management	10-Dec-20	4.6	, aka 'DirectX Graphics Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17137**	N/A	O-MIC-WIND-171220/859
Information Exposure	10-Dec-20	2.1	, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-17094. **CVE ID : CVE-2020-17138**	N/A	O-MIC-WIND-171220/860
N/A	10-Dec-20	4.6	, aka 'Windows Overlay Filter Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-17139**	N/A	O-MIC-WIND-171220/861
Information Exposure	10-Dec-20	4	, aka 'Windows SMB Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17140**	N/A	O-MIC-WIND-171220/862
windows_7					
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16958**	N/A	O-MIC-WIND-171220/863
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963,	N/A	O-MIC-WIND-171220/864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-16964. **CVE ID : CVE-2020-16959**		
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16960**	N/A	O-MIC-WIND-171220/865
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16961**	N/A	O-MIC-WIND-171220/866
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16962**	N/A	O-MIC-WIND-171220/867
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16964.	N/A	O-MIC-WIND-171220/868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16963		
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963. **CVE ID : CVE-2020-16964**	N/A	O-MIC-WIND-171220/869
N/A	10-Dec-20	2.1	, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17098**	N/A	O-MIC-WIND-171220/870
Information Exposure	10-Dec-20	4	, aka 'Windows SMB Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17140**	N/A	O-MIC-WIND-171220/871
windows_8.1					
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17092**	N/A	O-MIC-WIND-171220/872
N/A	10-Dec-20	9	, aka 'Windows NTFS Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17096**	N/A	O-MIC-WIND-171220/873
Improper Privilege Management	10-Dec-20	4.6	, aka 'Windows Digital Media Receiver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17097**	N/A	O-MIC-WIND-171220/874
N/A	10-Dec-20	2.1	, aka 'Windows GDI+ Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-171220/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-17098		
Information Exposure	10-Dec-20	4	, aka 'Windows SMB Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17140**	N/A	O-MIC-WIND-171220/876
windows_rt_8.1					
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17092**	N/A	O-MIC-WIND-171220/877
N/A	10-Dec-20	9	, aka 'Windows NTFS Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17096**	N/A	O-MIC-WIND-171220/878
Improper Privilege Management	10-Dec-20	4.6	, aka 'Windows Digital Media Receiver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17097**	N/A	O-MIC-WIND-171220/879
N/A	10-Dec-20	2.1	, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17098**	N/A	O-MIC-WIND-171220/880
Information Exposure	10-Dec-20	4	, aka 'Windows SMB Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17140**	N/A	O-MIC-WIND-171220/881
windows_server_2008					
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963,	N/A	O-MIC-WIND-171220/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-16964. **CVE ID : CVE-2020-16958**		
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16959**	N/A	O-MIC-WIND-171220/883
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16960**	N/A	O-MIC-WIND-171220/884
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16961**	N/A	O-MIC-WIND-171220/885
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16963, CVE-2020-16964.	N/A	O-MIC-WIND-171220/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16962		
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16964. **CVE ID : CVE-2020-16963**	N/A	O-MIC-WIND-171220/887
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963. **CVE ID : CVE-2020-16964**	N/A	O-MIC-WIND-171220/888
N/A	10-Dec-20	2.1	, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17098**	N/A	O-MIC-WIND-171220/889
Information Exposure	10-Dec-20	4	, aka 'Windows SMB Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17140**	N/A	O-MIC-WIND-171220/890
windows_server_2012					
N/A	10-Dec-20	4	, aka 'Kerberos Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16996**	N/A	O-MIC-WIND-171220/891
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-171220/892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-17092		
N/A	10-Dec-20	9	, aka 'Windows NTFS Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17096**	N/A	O-MIC-WIND-171220/893
Improper Privilege Management	10-Dec-20	4.6	, aka 'Windows Digital Media Receiver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17097**	N/A	O-MIC-WIND-171220/894
N/A	10-Dec-20	2.1	, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17098**	N/A	O-MIC-WIND-171220/895
Information Exposure	10-Dec-20	4	, aka 'Windows SMB Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17140**	N/A	O-MIC-WIND-171220/896
windows_server_2016					
Improper Privilege Management	10-Dec-20	4.6	, aka 'Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-17103, CVE-2020-17136. **CVE ID : CVE-2020-17134**	N/A	O-MIC-WIND-171220/897
Improper Privilege Management	10-Dec-20	4.6	, aka 'Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-17103, CVE-2020-17134. **CVE ID : CVE-2020-17136**	N/A	O-MIC-WIND-171220/898
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-	N/A	O-MIC-WIND-171220/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16958**		
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16959**	N/A	O-MIC-WIND-171220/900
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16960**	N/A	O-MIC-WIND-171220/901
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16961**	N/A	O-MIC-WIND-171220/902
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-	N/A	O-MIC-WIND-171220/903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			16961, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16962**		
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16964. **CVE ID : CVE-2020-16963**	N/A	O-MIC-WIND-171220/904
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963. **CVE ID : CVE-2020-16964**	N/A	O-MIC-WIND-171220/905
N/A	10-Dec-20	4	, aka 'Kerberos Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16996**	N/A	O-MIC-WIND-171220/906
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17092**	N/A	O-MIC-WIND-171220/907
N/A	10-Dec-20	2.1	, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-17138. **CVE ID : CVE-2020-17094**	N/A	O-MIC-WIND-171220/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Dec-20	9	, aka 'Hyper-V Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17095**	N/A	O-MIC-WIND-171220/909
N/A	10-Dec-20	9	, aka 'Windows NTFS Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17096**	N/A	O-MIC-WIND-171220/910
Improper Privilege Management	10-Dec-20	4.6	, aka 'Windows Digital Media Receiver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17097**	N/A	O-MIC-WIND-171220/911
N/A	10-Dec-20	2.1	, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17098**	N/A	O-MIC-WIND-171220/912
N/A	10-Dec-20	4.6	, aka 'Windows Lock Screen Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-17099**	N/A	O-MIC-WIND-171220/913
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-17134, CVE-2020-17136. **CVE ID : CVE-2020-17103**	N/A	O-MIC-WIND-171220/914
Improper Privilege Management	10-Dec-20	4.6	, aka 'DirectX Graphics Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17137**	N/A	O-MIC-WIND-171220/915
Information Exposure	10-Dec-20	2.1	, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-17094.	N/A	O-MIC-WIND-171220/916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-17138		
N/A	10-Dec-20	4.6	, aka 'Windows Overlay Filter Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-17139**	N/A	O-MIC-WIND-171220/917
Information Exposure	10-Dec-20	4	, aka 'Windows SMB Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17140**	N/A	O-MIC-WIND-171220/918
windows_server_2019					
Out-of-bounds Write	10-Dec-20	5.1	, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-17131**	N/A	O-MIC-WIND-171220/919
Improper Privilege Management	10-Dec-20	4.6	, aka 'Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-17103, CVE-2020-17136. **CVE ID : CVE-2020-17134**	N/A	O-MIC-WIND-171220/920
Improper Privilege Management	10-Dec-20	4.6	, aka 'Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-17103, CVE-2020-17134. **CVE ID : CVE-2020-17136**	N/A	O-MIC-WIND-171220/921
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964.	N/A	O-MIC-WIND-171220/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16958		
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16959**	N/A	O-MIC-WIND-171220/923
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16960**	N/A	O-MIC-WIND-171220/924
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16962, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16961**	N/A	O-MIC-WIND-171220/925
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16963, CVE-2020-16964. **CVE ID : CVE-2020-16962**	N/A	O-MIC-WIND-171220/926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16964. **CVE ID : CVE-2020-16963**	N/A	O-MIC-WIND-171220/927
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16958, CVE-2020-16959, CVE-2020-16960, CVE-2020-16961, CVE-2020-16962, CVE-2020-16963. **CVE ID : CVE-2020-16964**	N/A	O-MIC-WIND-171220/928
N/A	10-Dec-20	4	, aka 'Kerberos Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16996**	N/A	O-MIC-WIND-171220/929
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17092**	N/A	O-MIC-WIND-171220/930
N/A	10-Dec-20	2.1	, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-17138. **CVE ID : CVE-2020-17094**	N/A	O-MIC-WIND-171220/931
N/A	10-Dec-20	9	, aka 'Hyper-V Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17095**	N/A	O-MIC-WIND-171220/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Dec-20	9	, aka 'Windows NTFS Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17096**	N/A	O-MIC-WIND-171220/933
Improper Privilege Management	10-Dec-20	4.6	, aka 'Windows Digital Media Receiver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-17097**	N/A	O-MIC-WIND-171220/934
N/A	10-Dec-20	2.1	, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17098**	N/A	O-MIC-WIND-171220/935
N/A	10-Dec-20	4.6	, aka 'Windows Lock Screen Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-17099**	N/A	O-MIC-WIND-171220/936
Improper Privilege Management	10-Dec-20	7.2	, aka 'Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-17134, CVE-2020-17136. **CVE ID : CVE-2020-17103**	N/A	O-MIC-WIND-171220/937
N/A	10-Dec-20	4.6	, aka 'Windows Overlay Filter Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-17139**	N/A	O-MIC-WIND-171220/938
Information Exposure	10-Dec-20	4	, aka 'Windows SMB Information Disclosure Vulnerability'. **CVE ID : CVE-2020-17140**	N/A	O-MIC-WIND-171220/939
azure_devops_server					
Improper Input Validation	10-Dec-20	4.9	, aka 'Azure DevOps Server Spoofing Vulnerability'. **CVE ID : CVE-2020-17135**	N/A	O-MIC-AZUR-171220/940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	10-Dec-20	4.9	, aka 'Azure DevOps Server and Team Foundation Services Spoofing Vulnerability'. **CVE ID : CVE-2020-17145**	N/A	O-MIC-AZUR-171220/941
Mitsubishielectric					
le7-40gu-l_firmware					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**	N/A	O-MIT-LE7--171220/942
gt2107-wtbd_firmware					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all	N/A	O-MIT-GT21-171220/943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**		
gt2107-wtsd_firmware					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS)	N/A	O-MIT-GT21-171220/944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**		
gt2104-rtbd_firmware					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**	N/A	O-MIT-GT21-171220/945
gt2104-pmbd_firmware					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of	N/A	O-MIT-GT21-171220/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**		
gt2103-pmbd_firmware					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of	N/A	O-MIT-GT21-171220/947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the products may occur. **CVE ID : CVE-2020-5675**		
gs2110-wtbd_firmware					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**	N/A	O-MIT-GS21-171220/948
gs2107-wtbd_firmware					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-	N/A	O-MIT-GS21-171220/949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**		
NI					
compactrio_firmware					
Incorrect Permission Assignment for Critical Resource	11-Dec-20	7.8	Incorrect permissions are set by default for an API entry-point of a specific service, allowing a non-authenticated user to trigger a function that could reboot the CompactRIO (Driver versions prior to 20.5) remotely. **CVE ID : CVE-2020-25191**	N/A	O-NI-COMP-171220/950
Phoenixcontact					
btp_2043w_firmware					
Uncontrolled Resource Consumption	02-Dec-20	5	Uncontrolled Resource Consumption can be exploited to cause the Phoenix Contact HMIs BTP 2043W, BTP 2070W and BTP 2102W in all versions to become unresponsive and not accurately update the display content (Denial of	https://cert.vde.com/en-us/advisories/vde-2020-047	O-PHO-BTP_-171220/951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service). **CVE ID : CVE-2020-12524**		
btp_2070w_firmware					
Uncontrolled Resource Consumption	02-Dec-20	5	Uncontrolled Resource Consumption can be exploited to cause the Phoenix Contact HMIs BTP 2043W, BTP 2070W and BTP 2102W in all versions to become unresponsive and not accurately update the display content (Denial of Service). **CVE ID : CVE-2020-12524**	https://cert.vde.com/en-us/advisories/vde-2020-047	O-PHO-BTP_-171220/952
btp_2102w_firmware					
Uncontrolled Resource Consumption	02-Dec-20	5	Uncontrolled Resource Consumption can be exploited to cause the Phoenix Contact HMIs BTP 2043W, BTP 2070W and BTP 2102W in all versions to become unresponsive and not accurately update the display content (Denial of Service). **CVE ID : CVE-2020-12524**	https://cert.vde.com/en-us/advisories/vde-2020-047	O-PHO-BTP_-171220/953
plummac					
ik-401_firmware					
Insufficiently Protected Credentials	08-Dec-20	5	An improper webserver configuration on Plum IK-401 devices with firmware before 1.02 allows an attacker (with network access to the device) to obtain the configuration file, including hashed credential data. Successful exploitation	N/A	O-PLU-IK-4-171220/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow access to hashed credential data with a single unauthenticated GET request. **CVE ID : CVE-2020-28946**		
Qnap					
qts					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-20	4.3	This cross-site scripting vulnerability in Photo Station allows remote attackers to inject malicious code. QANP We have already fixed this vulnerability in the following versions of Photo Station. QTS 4.5.1: Photo Station 6.0.12 and later QTS 4.4.3: Photo Station 6.0.12 and later QTS 4.3.6: Photo Station 5.7.12 and later QTS 4.3.4: Photo Station 5.7.13 and later QTS 4.3.3: Photo Station 5.4.10 and later QTS 4.2.6: Photo Station 5.2.11 and later **CVE ID : CVE-2020-2491**	https://www.qnap.com/en/security-advisory/qsa-20-15	O-QNA-QTS-171220/955
Redhat					
enterprise_linux					
Divide By Zero	04-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/segment.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. This would most likely lead to an impact to application availability, but	N/A	O-RED-ENTE-171220/956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27765**		
Integer Overflow or Wraparound	04-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/quantum.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of types `float` and `unsigned char`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27767**	N/A	O-RED-ENTE-171220/957
Integer Overflow or Wraparound	04-Dec-20	4.3	In RestoreMSCWarning() of /coders/pdf.c there are several areas where calls to GetPixelIndex() could result in values outside the range of representable for the unsigned char type. The patch casts the return value of GetPixelIndex() to ssize_t type to avoid this bug. This undefined behavior could be triggered when ImageMagick processes a crafted pdf file. Red Hat Product Security marked	N/A	O-RED-ENTE-171220/958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this as Low severity because although it could potentially lead to an impact to application availability, no specific impact was demonstrated in this case. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27771**		
Integer Overflow or Wraparound	04-Dec-20	4.3	A flaw was found in ImageMagick in coders/bmp.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned int`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27772**	N/A	O-RED-ENTE-171220/959
Divide By Zero	04-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/gem-private.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned char` or division by zero. This would most likely lead	N/A	O-RED-ENTE-171220/960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27773**		
Integer Overflow or Wraparound	04-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/statistic.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of a too large shift for 64-bit type `ssize_t`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27774**	N/A	O-RED-ENTE-171220/961
Integer Overflow or Wraparound	04-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/quantum.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type unsigned char. This would most likely lead to an impact to application availability, but could potentially cause other	N/A	O-RED-ENTE-171220/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27775**		
Integer Overflow or Wraparound	04-Dec-20	4.3	A flaw was found in ImageMagick in MagickCore/statistic.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type unsigned long. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0. **CVE ID : CVE-2020-27776**	N/A	O-RED-ENTE-171220/963
Access of Uninitialized Pointer	03-Dec-20	5	A flaw was found in Poppler in the way certain PDF files were converted into HTML. A remote attacker could exploit this flaw by providing a malicious PDF file that, when processed by the 'pdftohtml' program, would crash the application causing a denial of service. **CVE ID : CVE-2020-27778**	N/A	O-RED-ENTE-171220/964
Improper Privilege Management	03-Dec-20	4	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use	N/A	O-RED-ENTE-171220/965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker. **CVE ID : CVE-2020-14318**		
Missing Release of Resource after Effective Lifetime	03-Dec-20	7.2	A flaw was found in libvirt, where it leaked a file descriptor for `/dev/mapper/control` into the QEMU process. This file descriptor allows for privileged operations to happen against the device-mapper on the host. This flaw allows a malicious guest user or process to perform operations outside of their standard permissions, potentially causing serious damage to the host operating system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2020-14339**	N/A	O-RED-ENTE-171220/966
Use After Free	03-Dec-20	4.6	A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker with permission to monitor perf events to corrupt memory and possibly escalate privileges. The highest threat from this vulnerability is to data confidentiality and integrity	N/A	O-RED-ENTE-171220/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as well as system availability. **CVE ID : CVE-2020-14351**		
N/A	02-Dec-20	4	A flaw was found in samba's DNS server. An authenticated user could use this flaw to the RPC server to crash. This RPC server, which also serves protocols other than dnsserver, will be restarted after a short delay, but it is easy for an authenticated non administrative attacker to crash it again as soon as it returns. The Samba DNS server itself will continue to operate, but many RPC services will not. **CVE ID : CVE-2020-14383**	N/A	O-RED-ENTE-171220/968
Use After Free	02-Dec-20	1.9	A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctls KDGKBSENT and KDSKBSENT. A local user could use this flaw to get read memory access out of bounds. The highest threat from this vulnerability is to data confidentiality. **CVE ID : CVE-2020-25656**	N/A	O-RED-ENTE-171220/969
NULL Pointer Dereference	08-Dec-20	5	A NULL pointer dereference was found in OpenLDAP server and was fixed in openldap 2.4.55, during a request for renaming RDNs. An unauthenticated attacker	https://bugzilla.redhat.com/show_bug.cgi?id=1894567	O-RED-ENTE-171220/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could remotely crash the slapd process by sending a specially crafted request, causing a Denial of Service. **CVE ID : CVE-2020-25692**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Dec-20	4.3	A XSS vulnerability was discovered in python-lxml's clean module. The module's parser didn't properly imitate browsers, which caused different behaviors between the sanitizer and the user's page. A remote attacker could exploit this flaw to run arbitrary HTML/JS code. **CVE ID : CVE-2020-27783**	N/A	O-RED-ENTE-171220/971
Use After Free	11-Dec-20	7.2	A flaw was found in the Linux kernels implementation of MIDI (kernel 5.7-rc6), where an attacker with a local account and the permissions to issue an ioctl commands to midi devices, could trigger a use-after-free. A write to this specific memory while freed and before use could cause the flow of execution to change and possibly allow for memory corruption or privilege escalation. **CVE ID : CVE-2020-27786**	N/A	O-RED-ENTE-171220/972
Concurrent Execution using Shared Resource with	11-Dec-20	5.4	A use-after-free flaw was found in kernel/trace/ring_buffer.c in Linux kernel (before 5.10-rc1). There was a race	N/A	O-RED-ENTE-171220/973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			problem in trace_open and resize of cpu buffer running parallely on different cpus, may cause a denial of service problem (DOS). This flaw could even allow a local attacker with special user privilege to a kernel information leak threat. **CVE ID : CVE-2020-27825**		
Out-of-bounds Write	06-Dec-20	5	sysdeps/i386/ldbl2mpn.c in the GNU C Library (aka glibc or libc6) before 2.23 on x86 targets has a stack-based buffer overflow if the input to any of the printf family of functions is an 80-bit long double with a non-canonical bit pattern, as seen when passing a \x00\x04\x00\x00\x00\x00\x00\x00\x00\x04 value to sprintf. NOTE: the issue does not affect glibc by default in 2016 or later (i.e., 2.23 or later) because of commits made in 2015 for inlining of C99 math functions through use of GCC built-ins. In other words, the reference to 2.23 is intentional despite the mention of "Fixed for glibc 2.33" in the 26649 reference. **CVE ID : CVE-2020-29573**	N/A	O-RED-ENTE-171220/974
Rockwellautomation					
micrologix_1100_b_firmware					
N/A	03-Dec-20	5	An exploitable denial-of-	N/A	O-ROC-MICR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service vulnerability exists in the IPv4 functionality of Allen-Bradley MicroLogix 1100 Programmable Logic Controller Systems Series B FRN 16.000, Series B FRN 15.002, Series B FRN 15.000, Series B FRN 14.000, Series B FRN 13.000, Series B FRN 12.000, Series B FRN 11.000 and Series B FRN 10.000. A specially crafted packet can cause a major error, resulting in a denial of service. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2020-6111**		171220/975
Schneider-electric					
140cpu65150_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-140C-171220/976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-140C-171220/977
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-140C-171220/978
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and	https://www.se.com/ww/en/download/document/SEVD-2020-343-	O-SCH-140C-171220/979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	03/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-140C-171220/980
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-140C-171220/981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**		
140cpu65160_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-140C-171220/982
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests.	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-140C-171220/983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7540		
140cpu65260_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	O-SCH-140C-171220/984
easergy_t300_firmware					
Missing Authorization	11-Dec-20	7.5	A CWE-862: Missing Authorization vulnerability exists in Easergy T300 (firmware 2.7 and older), that could cause a wide range of problems, including information exposures, denial of service, and arbitrary code execution when access control checks are not applied consistently. **CVE ID : CVE-2020-28215**	https://www.se.com/ww/en/download/document/SEVD-2020-315-06/	O-SCH-EASE-171220/985
Missing Encryption of Sensitive Data	11-Dec-20	5	A CWE-311: Missing Encryption of Sensitive Data vulnerability exists in Easergy T300 (firmware 2.7 and older), that would allow an attacker to read network traffic over HTTP protocol.	https://www.se.com/ww/en/download/document/SEVD-2020-315-06/	O-SCH-EASE-171220/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-28216		
Missing Encryption of Sensitive Data	11-Dec-20	5	A CWE-311: Missing Encryption of Sensitive Data vulnerability exists in Easergy T300 (firmware 2.7 and older), that would allow an attacker to read network traffic over HTTP protocol. **CVE ID : CVE-2020-28217**	https://www.se.com/ww/en/download/document/SEVD-2020-315-06/	O-SCH-EASE-171220/987
Improper Restriction of Rendered UI Layers or Frames	11-Dec-20	4.3	A CWE-1021: Improper Restriction of Rendered UI Layers or Frames vulnerability exists in Easergy T300 (firmware 2.7 and older), that would allow an attacker to trick a user into initiating an unintended action. **CVE ID : CVE-2020-28218**	https://www.se.com/ww/en/download/document/SEVD-2020-315-06/	O-SCH-EASE-171220/988
modicon_m258_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Dec-20	5.2	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Modicon M258 Firmware (All versions prior to V5.0.4.11) and SoMachine/SoMachine Motion software (All versions), that could cause a buffer overflow when the length of a file transferred to the webserver is not verified. **CVE ID : CVE-2020-28220**	https://www.se.com/ww/en/download/document/SEVD-2020-343-09/	O-SCH-MODI-171220/989
140noe77101_firmware					
Improper	11-Dec-20	5	A CWE-22: Improper	https://ww	O-SCH-140N-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	w.se.com/ww/en/download/document/SEVD-2020-343-05/	171220/990
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-140N-171220/991
140noe77111_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and	N/A	O-SCH-140N-171220/992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-140N-171220/993
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-140N-171220/994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**		
Missing Authenticati on for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-04/	O-SCH-140N-171220/995
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP.	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-03/	O-SCH-140N-171220/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7541		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-140N-171220/997
bmxnoc0401_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	O-SCH-BMXN-171220/998
Improper Check for Unusual or	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability	https://www.se.com/ww/en/down	O-SCH-BMXN-171220/999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	load/document/SEVD-2020-343-03/	
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-BMXN-171220/1000
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-BMXN-171220/1001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-BMXN-171220/1002
bmxnoe0100_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted	N/A	O-SCH-BMXN-171220/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP requests. **CVE ID : CVE-2020-7533**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-BMXN-171220/1004
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	O-SCH-BMXN-171220/1005
Improper	11-Dec-20	5	A CWE-754 Improper Check	https://ww	O-SCH-BMXN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Check for Unusual or Exceptional Conditions			for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	w.se.com/ww/en/download/document/SEVD-2020-343-03/	171220/1006
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-BMXN-171220/1007
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-BMXN-171220/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-BMXN-171220/1009
bmxnoe0110_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver	N/A	O-SCH-BMXN-171220/1010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-BMXN-171220/1011
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP.	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	O-SCH-BMXN-171220/1012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7536		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-BMXN-171220/1013
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-BMXN-171220/1014
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers	https://www.se.com/ww/en/download/document/SEVD-	O-SCH-BMXN-171220/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	2020-343-03/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-BMXN-171220/1016
bmxnor0200h_firmware					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	O-SCH-BMXN-171220/1017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**		
bmxp342020_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-BMXP-171220/1018
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	O-SCH-BMXP-171220/1019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1020
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-BMXP-171220/1021
Missing	11-Dec-20	7.5	A CWE-306: Missing	https://ww	O-SCH-BMXP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication for Critical Function			Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	w.se.com/ww/en/download/document/SEVD-2020-343-04/	171220/1022
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-BMXP-171220/1023
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1025
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-BMXP-171220/1026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP. **CVE ID : CVE-2020-7549**		
bmxp3420302_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	O-SCH-BMXP-171220/1027
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-BMXP-171220/1028
Improper	11-Dec-20	7.8	A CWE-754:Improper Check	https://ww	O-SCH-BMXP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Check for Unusual or Exceptional Conditions			for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	w.se.com/ww/en/download/document/SEVD-2020-343-07/	171220/1029
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1030
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-BMXP-171220/1031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**		
Missing Authenticati on for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-04/	O-SCH-BMXP-171220/1032
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-03/	O-SCH-BMXP-171220/1033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1034
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1035
Improper Check for Unusual or	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability	https://www.se.com/ww/en/down	O-SCH-BMXP-171220/1036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	load/document/SEVD-2020-343-06/	
bmxp342000_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	O-SCH-BMXP-171220/1037
Improper Limitation of a Pathname to a Restricted Directory ('Path	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-BMXP-171220/1038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	O-SCH-BMXP-171220/1039
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-BMXP-171220/1041
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-BMXP-171220/1042
Direct	11-Dec-20	5	A CWE-425: Direct Request	https://ww	O-SCH-BMXP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request ('Forced Browsing')			('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	w.se.com/ww/en/download/document/SEVD-2020-343-03/	171220/1043
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1044
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-BMXP-171220/1046
bmxp341000_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when	N/A	O-SCH-BMXP-171220/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-BMXP-171220/1048
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	O-SCH-BMXP-171220/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1050
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-BMXP-171220/1051
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum	https://www.se.com/ww/en/download/document/SEVD-2020-343-	O-SCH-BMXP-171220/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	04/	
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-BMXP-171220/1053
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1055
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-BMXP-171220/1056
bmxp3420102_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials	N/A	O-SCH-BMXP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**		171220/1057
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-BMXP-171220/1058
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon	https://www.se.com/ww/en/download/document/SEVD-2020-343-	O-SCH-BMXP-171220/1059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	07/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1060
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-BMXP-171220/1061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**		
Missing Authenticati on for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-04/	O-SCH-BMXP-171220/1062
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-03/	O-SCH-BMXP-171220/1063
Improper	11-Dec-20	5	A CWE-754: Improper Check	https://ww	O-SCH-BMXP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Check for Unusual or Exceptional Conditions			for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	w.se.com/ww/en/download/document/SEVD-2020-343-08/	171220/1064
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1065
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-BMXP-171220/1066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**		
tsxp574634_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	O-SCH-TSXP-171220/1067
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-TSXP-171220/1068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-TSXP-171220/1069
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-TSXP-171220/1070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authenticati on for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-04/	O-SCH-TSXP-171220/1071
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-03/	O-SCH-TSXP-171220/1072
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-08/	O-SCH-TSXP-171220/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-TSXP-171220/1074
tsxp575634_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver	N/A	O-SCH-TSXP-171220/1075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-TSXP-171220/1076
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-TSXP-171220/1077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-TSXP-171220/1078
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-TSXP-171220/1079
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and	https://www.se.com/ww/en/download/document/SEVD-2020-343-	O-SCH-TSXP-171220/1080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	03/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-TSXP-171220/1081
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-TSXP-171220/1082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**		
tsxp576634_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	O-SCH-TSXP-171220/1083
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP.	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-TSXP-171220/1084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7535		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-TSXP-171220/1085
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-TSXP-171220/1086
Missing Authentication for Critical	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy	https://www.se.com/ww/en/download/document/SEVD-	O-SCH-TSXP-171220/1087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	2020-343-04/	
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-TSXP-171220/1088
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-TSXP-171220/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-TSXP-171220/1090
tsxety4103_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	O-SCH-TSXE-171220/1091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-TSXE-171220/1092
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-TSXE-171220/1093
Missing Authentication for Critical	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on	https://www.se.com/ww/en/download/docum	O-SCH-TSXE-171220/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	ent/SEVD-2020-343-04/	
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-TSXE-171220/1095
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-TSXE-171220/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**		
tsxety5103_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	O-SCH-TSXE-171220/1097
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-TSXE-171220/1098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controller over HTTP. **CVE ID : CVE-2020-7535**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-TSXE-171220/1099
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-TSXE-171220/1100
Direct Request ('Forced	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the	https://www.se.com/ww/en/down	O-SCH-TSXE-171220/1101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Browsing')			Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	load/document/SEVD-2020-343-03/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-TSXE-171220/1102
140noc78000_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules	N/A	O-SCH-140N-171220/1103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-140N-171220/1104
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-140N-171220/1105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**		
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-140N-171220/1106
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-140N-171220/1107
Improper Check for	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional	https://www.se.com/w	O-SCH-140N-171220/1108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unusual or Exceptional Conditions			Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	w/en/download/document/SEVD-2020-343-06/	
140noc77101_firmware					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	O-SCH-140N-171220/1109
Improper Limitation of a Pathname to a Restricted Directory ('Path	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers	https://www.se.com/ww/en/download/document/SEVD-2020-343-	O-SCH-140N-171220/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	05/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-140N-171220/1111
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-140N-171220/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**		
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-140N-171220/1113
bmxp3420102cl_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-BMXP-171220/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controller over HTTP. **CVE ID : CVE-2020-7535**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	O-SCH-BMXP-171220/1115
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1116
Improper Check for Unusual or	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability	https://www.se.com/ww/en/down	O-SCH-BMXP-171220/1117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	load/document/SEVD-2020-343-03/	
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-BMXP-171220/1118
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-BMXP-171220/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1120
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller.	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7543		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-BMXP-171220/1122
bmxp3420302cl_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-BMXP-171220/1123
Improper	11-Dec-20	7.8	A CWE-754:Improper Check	https://ww	O-SCH-BMXP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Check for Unusual or Exceptional Conditions			for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	w.se.com/ww/en/download/document/SEVD-2020-343-07/	171220/1124
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1125
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	O-SCH-BMXP-171220/1126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**		
Missing Authenticati on for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-04/	O-SCH-BMXP-171220/1127
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-03/	O-SCH-BMXP-171220/1128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1129
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMXP-171220/1130
Improper Check for Unusual or	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability	https://www.se.com/ww/en/down	O-SCH-BMXP-171220/1131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	load/document/SEVD-2020-343-06/	
140noc78100_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	O-SCH-140N-171220/1132
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum	https://www.se.com/ww/en/download/document/SEVD-2020-343-	O-SCH-140N-171220/1133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	03/	
Missing Authenticati on for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-04/	O-SCH-140N-171220/1134
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-03/	O-SCH-140N-171220/1135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	O-SCH-140N-171220/1136
bmep584040_firmware					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1138
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1139
bmep582040_firmware					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon	https://www.se.com/ww/en/download/document/SEVD-2020-343-	O-SCH-BMEP-171220/1140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	08/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1141
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**		
bmep586040_firmware					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1143
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1144
Improper Check for	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional	https://www.se.com/w	O-SCH-BMEP-171220/1145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unusual or Exceptional Conditions			Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	w/en/download/document/SEVD-2020-343-08/	
bmep585040_firmware					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1146
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1148
bmep582020_firmware					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controller. **CVE ID : CVE-2020-7537**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1150
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1151
bmep581020_firmware					
Improper Check for Unusual or	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability	https://www.se.com/ww/en/down	O-SCH-BMEP-171220/1152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	load/document/SEVD-2020-343-08/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1153
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**		
bmep584020_firmware					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1155
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller.	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7542		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1157
bmep583040_firmware					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1158
Improper Check for Unusual or Exceptional	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580,	https://www.se.com/ww/en/download/docum	O-SCH-BMEP-171220/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conditions			Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	ent/SEVD-2020-343-08/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1160
bmep583020_firmware					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1162
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	O-SCH-BMEP-171220/1163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bmxnor200h_firmware					
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	O-SCH-BMXN-171220/1164
acti9_smartlink_si_d_firmware					
Use of Insufficiently Random Values	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login. **CVE ID : CVE-2020-7548**	N/A	O-SCH-ACTI-171220/1165
acti9_smartlink_si_b_firmware					
Use of Insufficiently Random Values	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login.	N/A	O-SCH-ACTI-171220/1166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7548		
acti9_powertag_link_firmware					
Use of Insufficiently Random Values	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login. **CVE ID : CVE-2020-7548**	N/A	O-SCH-ACTI-171220/1167
acti9_powertag_link_hd_firmware					
Use of Insufficiently Random Values	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login. **CVE ID : CVE-2020-7548**	N/A	O-SCH-ACTI-171220/1168
acti9_smartlink_el_b_firmware					
Use of Insufficiently Random Values	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login. **CVE ID : CVE-2020-7548**	N/A	O-SCH-ACTI-171220/1169
wiser_link_firmware					
Use of Insufficiently	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random	N/A	O-SCH-WISE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Random Values			Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login. **CVE ID : CVE-2020-7548**		171220/1170
wiser_energy_firmware					
Use of Insufficiently Random Values	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login. **CVE ID : CVE-2020-7548**	N/A	O-SCH-WISE-171220/1171
Singtel					
askey_ap5100w-d171_firmware					
Weak Password Requirements	10-Dec-20	10	Askey AP5100W_Dual_SIG_1.01.097 and all prior versions use a weak password at the Operating System (rlx-linux) level. This allows an attacker to gain unauthorized access as an admin or root user to the device Operating System via Telnet or SSH. **CVE ID : CVE-2020-26201**	https://www.askey.com.tw/incident_report_notifications.html	O-SIN-ASKE-171220/1172
Sophos					
cyberoamos					
Improper Neutralization of Special	11-Dec-20	7.5	An SQL injection vulnerability in the WebAdmin of Cyberoam OS	N/A	O-SOP-CYBE-171220/1173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			through 2020-12-04 allows unauthenticated attackers to execute arbitrary SQL statements remotely. **CVE ID : CVE-2020-29574**		
Wago					
750-352_firmware					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	O-WAG-750--171220/1174
750-829_firmware					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	O-WAG-750--171220/1175
750-831_firmware					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	O-WAG-750--171220/1176
750-852_firmware					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable	https://cert.vde.com/en-us/advisori	O-WAG-750--171220/1177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for a special denial of service attack. **CVE ID : CVE-2020-12516**	es/vde-2020-042	
750-880_firmware					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	O-WAG-750--171220/1178
750-881_firmware					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	O-WAG-750--171220/1179
750-882_firmware					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	O-WAG-750--171220/1180
750-885_firmware					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	O-WAG-750--171220/1181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
750-889_firmware					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	O-WAG-750--171220/1182
750-331_firmware					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	O-WAG-750--171220/1183
westerndigital					
my_cloud_os_5					
N/A	01-Dec-20	7.5	On Western Digital My Cloud OS 5 devices before 5.06.115, the NAS Admin dashboard has an authentication bypass vulnerability that could allow an unauthenticated user to execute privileged commands on the device. **CVE ID : CVE-2020-28940**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	O-WES-MY_C-171220/1184
N/A	01-Dec-20	7.5	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.06.115. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to execute privileged commands on the device via a cookie. (In addition, an	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	O-WES-MY_C-171220/1185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			upload endpoint could then be used by an authenticated administrator to upload executable PHP scripts.) **CVE ID : CVE-2020-28970**		
Improper Input Validation	01-Dec-20	7.5	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.06.115. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to execute privileged commands on the device via a cookie, because of insufficient validation of URI paths. **CVE ID : CVE-2020-28971**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	O-WES-MY_C-171220/1186
ZTE					
zxv10_w908_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Dec-20	7.5	A ZXELINK wireless controller has a SQL injection vulnerability. A remote attacker does not need to log in. By sending malicious SQL statements, because the device does not properly filter parameters, successful use can obtain management rights. This affects: ZXV10 W908 all versions before MIPS_A_1022IPV6R3T6P7Y20. **CVE ID : CVE-2020-6880**	N/A	O-ZTE-ZXV1-171220/1187
Hardware					
Arubanetworks					
7005					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7005-171220/1188
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7005-171220/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.7.0.0 and below. **CVE ID : CVE-2020-24634**		
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7005-171220/1190
7008					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7008-171220/1191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7008-171220/1192
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7008-171220/1193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**		
7010					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7010-171220/1194
Improper Neutralization of Special	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending	https://support.hpe.com/hpsc/do	H-ARU-7010-171220/1195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**	c/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7010-171220/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-24637		
7024					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7024-171220/1197
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7024-171220/1198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**		
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7024-171220/1199
7030					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04	H-ARU-7030-171220/1200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**	072en_us	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7030-171220/1201
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=e	H-ARU-7030-171220/1202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**	mr_na-hpesbnw04072en_us	
7205					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7205-171220/1203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7205-171220/1204
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7205-171220/1205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**		
7210					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7210-171220/1206
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7210-171220/1207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**		
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7210-171220/1208
7220					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-ARU-7220-171220/1209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**	hpesbnw04072en_us	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7220-171220/1210
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful	https://support.hpe.com/hpsc/doc/public/display?docL	H-ARU-7220-171220/1211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**	ocale=en_US&docId=emr_na-hpesbnw04072en_us	
7240xm					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7240-171220/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.7.0.0 and below. **CVE ID : CVE-2020-24633**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7240-171220/1213
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7240-171220/1214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**		
7280					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7280-171220/1215
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04	H-ARU-7280-171220/1216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**	072en_us	
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-7280-171220/1217
9004					
Buffer Copy without Checking Size of Input ('Classic	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending	https://support.hpe.com/hpsc/doc/public/display?docL	H-ARU-9004-171220/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**	ocale=en_US&docId=emr_na-hpesbnw04072en_us	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-9004-171220/1219
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2	https://support.hpe.co	H-ARU-9004-171220/1220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**	m/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	
9004-lte					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-9004-171220/1221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-9004-171220/1222
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-9004-171220/1223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**		
9012					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Dec-20	10	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24633**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-9012-171220/1224
Improper Neutralization of Special Elements used in a Command ('Command	11-Dec-20	10	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=e	H-ARU-9012-171220/1225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24634**	mr_na-hpesbnw04072en_us	
N/A	11-Dec-20	9	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below. **CVE ID : CVE-2020-24637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04072en_us	H-ARU-9012-171220/1226
askey					
ap5100w					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Insufficiently Random Values	11-Dec-20	4.3	Askey AP5100W devices through AP5100W_Dual_SIG_1.01.097 are affected by WPS PIN offline brute-force cracking. This arises because of issues with the random number selection for the Diffie-Hellman exchange. By capturing an attempted (and even failed) WPS authentication attempt, it is possible to brute force the overall authentication exchange. This allows an attacker to obtain the recovered WPS PIN in minutes or even seconds, and eventually obtain the Wi-Fi PSK key, gaining access to the Wi=Fi network. **CVE ID : CVE-2020-15023**	https://www.askey.com.tw/incident_report_notifications.html	H-ASK-AP51-171220/1227
N/A	11-Dec-20	10	Network Analysis functionality in Askey AP5100W_Dual_SIG_1.01.097 and all prior versions allows remote attackers to execute arbitrary commands via a shell metacharacter in the ping, traceroute, or route options. **CVE ID : CVE-2020-15357**	N/A	H-ASK-AP51-171220/1228
Asus					
rt-ac88u					
Improper Neutralization of Special Elements in	09-Dec-20	5	An injection vulnerability exists in RT-AC88U Download Master before 3.1.0.108. Accessing	N/A	H-ASU-RT-A-171220/1229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Output Used by a Downstream Component ('Injection')			Main_Login.asp?flag=1&productname=FOOBAR&url=/downloadmaster/task.asp will redirect to the login site, which will show the value of the parameter productname within the title. An attacker might be able to influence the appearance of the login page, aka text injection. **CVE ID : CVE-2020-29655**		
Information Exposure	09-Dec-20	5	An information disclosure vulnerability exists in RT-AC88U Download Master before 3.1.0.108. A direct access to /downloadmaster/dm_apply.cgi?action_mode=initial&download_type=General&special_cgi=get_language makes it possible to reach "unknown functionality" in a "known to be easy" manner via an unspecified "public exploit." **CVE ID : CVE-2020-29656**	N/A	H-ASU-RT-A-171220/1230
atx					
minicmts200a					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Dec-20	5	A Directory Traversal vulnerability exists in ATX miniCMTS200a Broadband Gateway through 2.0 and Pico CMTS through 2.0. Successful exploitation of this vulnerability would allow an unauthenticated attacker to retrieve administrator credentials by sending a malicious POST	N/A	H-ATX-MINI-171220/1231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request. **CVE ID : CVE-2020-28993**		
Edimax					
ic-3116w					
Out-of-bounds Write	01-Dec-20	7.5	A stack-based buffer-overflow exists in Edimax IP-Camera IC-3116W (v3.06) and IC-3140W (v3.07), which allows an unauthenticated, unauthorized attacker to perform remote-code-execution due to a crafted GET-Request. The overflow occurs in binary ipcam_cgi due to a missing type check in function doGetSysteminfo(). This has been fixed in version: IC-3116W v3.08. **CVE ID : CVE-2020-26762**	https://www.edimax.com/edimax/download/download/data/edimax/de/download/for_home/home_network_cameras/home_network_cameras_indoor_fixed/ic-3116w	H-EDI-IC-3-171220/1232
ic-3140w					
Out-of-bounds Write	01-Dec-20	7.5	A stack-based buffer-overflow exists in Edimax IP-Camera IC-3116W (v3.06) and IC-3140W (v3.07), which allows an unauthenticated, unauthorized attacker to perform remote-code-execution due to a crafted GET-Request. The overflow occurs in binary ipcam_cgi due to a missing type check in function doGetSysteminfo(). This has been fixed in version: IC-3116W v3.08.	https://www.edimax.com/edimax/download/download/data/edimax/de/download/for_home/home_network_cameras/home_network_cameras_indoor_fixed/ic-3116w	H-EDI-IC-3-171220/1233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-26762		
Huawei					
honor_20_pro					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	H-HUA-HONO-171220/1234
yale-l61a					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a	N/A	H-HUA-YALE-171220/1235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
hima-l29c					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	H-HUA-HIMA-171220/1236
sydneym-al00					
Out-of-	01-Dec-20	4.6	HUAWEI nova 4 versions	N/A	H-HUA-SYDN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			earlier than 10.0.0.165(C01E34R2P4) and SydneyM-AL00 versions earlier than 10.0.0.165(C00E66R1P5) have an out-of-bounds read and write vulnerability. An attacker with specific permissions crafts malformed packet with specific parameter and sends the packet to the affected products. Due to insufficient validation of packet, which may be exploited to cause the information leakage or arbitrary code execution. **CVE ID : CVE-2020-9117**		171220/1237
yale-tl00b					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP,	N/A	H-HUA-YALE-171220/1238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
yalep-al10b					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	H-HUA-YALE-171220/1239
laya-al00ep					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker	N/A	H-HUA-LAYA-171220/1240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
princeton-al10b					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	H-HUA-PRIN-171220/1241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tony-al00b					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	H-HUA-TONY-171220/1242
mate_20_pro					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code	N/A	H-HUA-MATE-171220/1243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
p30_pro					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	H-HUA-P30_-171220/1244
p30					
Buffer Copy without Checking Size of Input	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently	N/A	H-HUA-P30-171220/1245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
mate_20_x					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP,	N/A	H-HUA-MATE-171220/1246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**		
mate_20					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-20	6.8	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B. **CVE ID : CVE-2020-9247**	N/A	H-HUA-MATE-171220/1247
nova_4					
Out-of-bounds Write	01-Dec-20	4.6	HUAWEI nova 4 versions earlier than 10.0.0.165(C01E34R2P4) and SydneyM-AL00 versions earlier than 10.0.0.165(C00E66R1P5) have an out-of-bounds read and write vulnerability. An attacker with specific	N/A	H-HUA-NOVA-171220/1248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permissions crafts malformed packet with specific parameter and sends the packet to the affected products. Due to insufficient validation of packet, which may be exploited to cause the information leakage or arbitrary code execution. **CVE ID : CVE-2020-9117**		
inspur					
ns5162m5					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	H-INS-NS51-171220/1249
ns5488m5					
Improper Verification of Cryptographi	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator	https://en.inspur.com/en/security_bulletins/s	H-INS-NS54-171220/1250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c Signature			privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	ecurity_advisory2/2543921/index.html	
ns5484m5					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	H-INS-NS54-171220/1251
ns5482m5					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	H-INS-NS54-171220/1252
nf5280m5					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	H-INS-NF52-171220/1253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			upgrade the BMC. **CVE ID : CVE-2020-26122**		
nf5468m5					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	H-INS-NF54-171220/1254
nf5488m5-d					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	H-INS-NF54-171220/1255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**		
nf5180m5					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	H-INS-NF51-171220/1256
nf5270m5					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	H-INS-NF52-171220/1257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**		
nf5260m5					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	H-INS-NF52-171220/1258
nf5266m5					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller	https://en.inspur.com/en/security_bulletins/security_advisory2/2543	H-INS-NF52-171220/1259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	921/index.html	
nf5466m5					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	H-INS-NF54-171220/1260
nf5486m5					
Improper Verification	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5	https://en.inspur.com/	H-INS-NF54-171220/1261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Cryptographic Signature			devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	en/security_bulletins/security_advisory2/2543921/index.html	
nf8480m5					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	H-INS-NF84-171220/1262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nf8260m5					
Improper Verification of Cryptographic Signature	07-Dec-20	6.5	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC. **CVE ID : CVE-2020-26122**	https://en.inspur.com/en/security_bulletins/security_advisory2/2543921/index.html	H-INS-NF82-171220/1263
kia					
head_unit					
Incorrect Default Permissions	01-Dec-20	4.6	Kia Motors Head Unit with Software version: SOP.003.30.18.0703, SOP.005.7.181019, and SOP.007.1.191209 may allow an attacker to inject unauthorized commands, by executing the micomd executable deamon, to trigger unintended functionalities. In addition, this executable may be used by an attacker to inject commands to generate CAN frames that are sent into the M-CAN bus (Multimedia CAN	N/A	H-KIA-HEAD-171220/1264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bus) of the vehicle. **CVE ID : CVE-2020-8539**		
Mitsubishielectric					
le7-40gu-l					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**	N/A	H-MIT-LE7--171220/1265
gt2107-wtbd					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD	N/A	H-MIT-GT21-171220/1266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**		
gt2107-wtsd					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur.	N/A	H-MIT-GT21-171220/1267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5675		
gt2104-rtbd					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**	N/A	H-MIT-GT21-171220/1268
gt2104-pmbd					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-	N/A	H-MIT-GT21-171220/1269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**		
gt2103-pmbd					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**	N/A	H-MIT-GT21-171220/1270
gs2110-wtbd					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**	N/A	H-MIT-GS21-171220/1271
gs2107-wtbd					
Out-of-bounds Read	04-Dec-20	5	Out-of-bounds read issue in GT21 model of GOT2000 series (GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, and GT2103-PMBD all versions), GS21 model of GOT series (GS2110-WTBD all versions and GS2107-WTBD all versions), and Tension Controller LE7-40GU-L all versions allows a remote attacker to cause a	N/A	H-MIT-GS21-171220/1272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur. **CVE ID : CVE-2020-5675**		
Netscout					
sensor6-r2s1-e					
Improper Privilege Management	03-Dec-20	9.3	NETSCOUT AirMagnet Enterprise 11.1.4 build 37257 and earlier has a sensor escalated privileges vulnerability that can be exploited to provide someone with administrative access to a sensor, with credentials to invoke a command to provide root access to the operating system. The attacker must complete a straightforward password-cracking exercise. **CVE ID : CVE-2020-28251**	https://www.netscout.com/securityadvisories	H-NET-SENS-171220/1273
sensor6-r2s1-i					
Improper Privilege Management	03-Dec-20	9.3	NETSCOUT AirMagnet Enterprise 11.1.4 build 37257 and earlier has a sensor escalated privileges vulnerability that can be exploited to provide someone with administrative access to a sensor, with credentials to	https://www.netscout.com/securityadvisories	H-NET-SENS-171220/1274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			invoke a command to provide root access to the operating system. The attacker must complete a straightforward password-cracking exercise. **CVE ID : CVE-2020-28251**		
sensor4-r1s1w1-e					
Improper Privilege Management	03-Dec-20	9.3	NETSCOUT AirMagnet Enterprise 11.1.4 build 37257 and earlier has a sensor escalated privileges vulnerability that can be exploited to provide someone with administrative access to a sensor, with credentials to invoke a command to provide root access to the operating system. The attacker must complete a straightforward password-cracking exercise. **CVE ID : CVE-2020-28251**	https://www.netscout.com/securityadvisories	H-NET-SENS-171220/1275
sensor4-r2s1-e					
Improper Privilege Management	03-Dec-20	9.3	NETSCOUT AirMagnet Enterprise 11.1.4 build 37257 and earlier has a sensor escalated privileges vulnerability that can be exploited to provide someone with administrative access to a sensor, with credentials to invoke a command to provide root access to the operating system. The attacker must complete a	https://www.netscout.com/securityadvisories	H-NET-SENS-171220/1276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			straightforward password-cracking exercise. **CVE ID : CVE-2020-28251**		
sensor4-r2s1-i					
Improper Privilege Management	03-Dec-20	9.3	NETSCOUT AirMagnet Enterprise 11.1.4 build 37257 and earlier has a sensor escalated privileges vulnerability that can be exploited to provide someone with administrative access to a sensor, with credentials to invoke a command to provide root access to the operating system. The attacker must complete a straightforward password-cracking exercise. **CVE ID : CVE-2020-28251**	https://www.netscout.com/securityadvisories	H-NET-SENS-171220/1277
sensor6-r1s0w1-e					
Improper Privilege Management	03-Dec-20	9.3	NETSCOUT AirMagnet Enterprise 11.1.4 build 37257 and earlier has a sensor escalated privileges vulnerability that can be exploited to provide someone with administrative access to a sensor, with credentials to invoke a command to provide root access to the operating system. The attacker must complete a straightforward password-cracking exercise. **CVE ID : CVE-2020-28251**	https://www.netscout.com/securityadvisories	H-NET-SENS-171220/1278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NI					
compactrio					
Incorrect Permission Assignment for Critical Resource	11-Dec-20	7.8	Incorrect permissions are set by default for an API entry-point of a specific service, allowing a non-authenticated user to trigger a function that could reboot the CompactRIO (Driver versions prior to 20.5) remotely. **CVE ID : CVE-2020-25191**	N/A	H-NI-COMP-171220/1279
Phoenixcontact					
btp_2043w					
Uncontrolled Resource Consumption	02-Dec-20	5	Uncontrolled Resource Consumption can be exploited to cause the Phoenix Contact HMIs BTP 2043W, BTP 2070W and BTP 2102W in all versions to become unresponsive and not accurately update the display content (Denial of Service). **CVE ID : CVE-2020-12524**	https://cert.vde.com/en-us/advisories/vde-2020-047	H-PHO-BTP_-171220/1280
btp_2070w					
Uncontrolled Resource Consumption	02-Dec-20	5	Uncontrolled Resource Consumption can be exploited to cause the Phoenix Contact HMIs BTP 2043W, BTP 2070W and BTP 2102W in all versions to become unresponsive and not accurately update the display content (Denial of Service). **CVE ID : CVE-2020-12524**	https://cert.vde.com/en-us/advisories/vde-2020-047	H-PHO-BTP_-171220/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
btp_2102w					
Uncontrolled Resource Consumption	02-Dec-20	5	Uncontrolled Resource Consumption can be exploited to cause the Phoenix Contact HMIs BTP 2043W, BTP 2070W and BTP 2102W in all versions to become unresponsive and not accurately update the display content (Denial of Service). **CVE ID : CVE-2020-12524**	https://cert.vde.com/en-us/advisories/vde-2020-047	H-PHO-BTP_-171220/1282
plummac					
ik-401					
Insufficiently Protected Credentials	08-Dec-20	5	An improper webserver configuration on Plum IK-401 devices with firmware before 1.02 allows an attacker (with network access to the device) to obtain the configuration file, including hashed credential data. Successful exploitation could allow access to hashed credential data with a single unauthenticated GET request. **CVE ID : CVE-2020-28946**	N/A	H-PLU-IK-4-171220/1283
Rockwellautomation					
micrologix_1100					
N/A	03-Dec-20	5	An exploitable denial-of-service vulnerability exists in the IPv4 functionality of Allen-Bradley MicroLogix 1100 Programmable Logic Controller Systems Series B FRN 16.000, Series B FRN	N/A	H-ROC-MICR-171220/1284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15.002, Series B FRN 15.000, Series B FRN 14.000, Series B FRN 13.000, Series B FRN 12.000, Series B FRN 11.000 and Series B FRN 10.000. A specially crafted packet can cause a major error, resulting in a denial of service. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2020-6111**		
Schneider-electric					
140cpu65150					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-140C-171220/1285
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum	https://www.se.com/ww/en/download/document/SEVD-2020-343-	H-SCH-140C-171220/1286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	03/	
Missing Authenticati on for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-04/	H-SCH-140C-171220/1287
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-03/	H-SCH-140C-171220/1288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-140C-171220/1289
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-140C-171220/1290
140cpu65160					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-140C-171220/1291
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-140C-171220/1292
140cpu65260					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon	N/A	H-SCH-140C-171220/1293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**		
easergy_t300					
Missing Authorization	11-Dec-20	7.5	A CWE-862: Missing Authorization vulnerability exists in Easergy T300 (firmware 2.7 and older), that could cause a wide range of problems, including information exposures, denial of service, and arbitrary code execution when access control checks are not applied consistently. **CVE ID : CVE-2020-28215**	https://www.se.com/ww/en/download/document/SEVD-2020-315-06/	H-SCH-EASE-171220/1294
Missing Encryption of Sensitive Data	11-Dec-20	5	A CWE-311: Missing Encryption of Sensitive Data vulnerability exists in Easergy T300 (firmware 2.7 and older), that would allow an attacker to read network traffic over HTTP protocol. **CVE ID : CVE-2020-28216**	https://www.se.com/ww/en/download/document/SEVD-2020-315-06/	H-SCH-EASE-171220/1295
Missing Encryption of Sensitive Data	11-Dec-20	5	A CWE-311: Missing Encryption of Sensitive Data vulnerability exists in Easergy T300 (firmware 2.7 and older), that would allow	https://www.se.com/ww/en/download/document/SEVD-	H-SCH-EASE-171220/1296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an attacker to read network traffic over HTTP protocol. **CVE ID : CVE-2020-28217**	2020-315-06/	
Improper Restriction of Rendered UI Layers or Frames	11-Dec-20	4.3	A CWE-1021: Improper Restriction of Rendered UI Layers or Frames vulnerability exists in Easergy T300 (firmware 2.7 and older), that would allow an attacker to trick a user into initiating an unintended action. **CVE ID : CVE-2020-28218**	https://www.se.com/ww/en/download/document/SEVD-2020-315-06/	H-SCH-EASE-171220/1297
140noe77101					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-140N-171220/1298
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum	https://www.se.com/ww/en/download/document/SEVD-2020-343-	H-SCH-140N-171220/1299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	04/	
140noe77111					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	H-SCH-140N-171220/1300
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-140N-171220/1301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-140N-171220/1302
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests.	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-140N-171220/1303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7540		
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-140N-171220/1304
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-140N-171220/1305
bmxp341000					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on	N/A	H-SCH-BMXP-171220/1306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-BMXP-171220/1307
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	H-SCH-BMXP-171220/1308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1309
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXP-171220/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sent to the controller over HTTP. **CVE ID : CVE-2020-7539**		
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-BMXP-171220/1311
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXP-171220/1312
Improper Check for Unusual or	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability	https://www.se.com/ww/en/down	H-SCH-BMXP-171220/1313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	load/document/SEVD-2020-343-08/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1314
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-BMXP-171220/1315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**		
bmxp342000					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	H-SCH-BMXP-171220/1316
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-BMXP-171220/1317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	H-SCH-BMXP-171220/1318
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1319
Improper Check for	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional	https://www.se.com/w	H-SCH-BMXP-171220/1320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unusual or Exceptional Conditions			Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	w/en/download/document/SEVD-2020-343-03/	
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-BMXP-171220/1321
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXP-171220/1322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1323
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller.	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7543		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-BMXP-171220/1325
bmxp3420102					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	H-SCH-BMXP-171220/1326
Improper Limitation of a Pathname	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path	https://www.se.com/ww/en/down	H-SCH-BMXP-171220/1327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	load/document/SEVD-2020-343-05/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	H-SCH-BMXP-171220/1328
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXP-171220/1330
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-BMXP-171220/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when sending special HTTP requests. **CVE ID : CVE-2020-7540**		
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXP-171220/1332
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1333
Improper Check for Unusual or	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability	https://www.se.com/ww/en/down	H-SCH-BMXP-171220/1334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	load/document/SEVD-2020-343-08/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-BMXP-171220/1335
bmxp3420102cl					
Improper Limitation of a Pathname to a Restricted Directory ('Path	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-BMXP-171220/1336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	H-SCH-BMXP-171220/1337
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXP-171220/1339
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-BMXP-171220/1340
Direct	11-Dec-20	5	A CWE-425: Direct Request	https://ww	H-SCH-BMXP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request ('Forced Browsing')			('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	w.se.com/ww/en/download/document/SEVD-2020-343-03/	171220/1341
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1342
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-BMXP-171220/1344
bmxp342020					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-BMXP-171220/1345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	H-SCH-BMXP-171220/1346
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXP-171220/1348
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-BMXP-171220/1349
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and	https://www.se.com/ww/en/download/document/SEVD-2020-343-	H-SCH-BMXP-171220/1350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	03/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1351
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-BMXP-171220/1353
bmxp3420302					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	H-SCH-BMXP-171220/1354
Improper	11-Dec-20	5	A CWE-22: Improper	https://ww	H-SCH-BMXP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	w.se.com/ww/en/download/document/SEVD-2020-343-05/	171220/1355
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	H-SCH-BMXP-171220/1356
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy	https://www.se.com/ww/en/download/document/SEVD-	H-SCH-BMXP-171220/1357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	2020-343-08/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXP-171220/1358
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-BMXP-171220/1359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**		
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXP-171220/1360
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1361
Improper	11-Dec-20	5	A CWE-754: Improper Check	https://ww	H-SCH-BMXP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Check for Unusual or Exceptional Conditions			for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	w.se.com/ww/en/download/document/SEVD-2020-343-08/	171220/1362
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-BMXP-171220/1363
bmxp3420302cl					
Improper Limitation of a Pathname to a Restricted Directory	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon	https://www.se.com/ww/en/download/document/SEVD-2020-343-	H-SCH-BMXP-171220/1364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	05/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	H-SCH-BMXP-171220/1365
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXP-171220/1367
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests.	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-BMXP-171220/1368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7540		
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXP-171220/1369
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMXP-171220/1370
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon	https://www.se.com/ww/en/download/document/SEVD-2020-343-	H-SCH-BMXP-171220/1371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	08/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-BMXP-171220/1372
bmep581020					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1374
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1375
bmep582020					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1376
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1377
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**		
bmep582040					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1379
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1381
bmep583020					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1382
Improper Check for	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional	https://www.se.com/w	H-SCH-BMEP-171220/1383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unusual or Exceptional Conditions			Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	w/en/download/document/SEVD-2020-343-08/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1384
bmep583040					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1386
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller.	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7543		
bmep584020					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1388
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1389
Improper Check for Unusual or Exceptional	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580,	https://www.se.com/ww/en/download/docum	H-SCH-BMEP-171220/1390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conditions			Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	ent/SEVD-2020-343-08/	
bmep584040					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1391
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1393
bmep585040					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller.	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7537		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1395
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1396
bmep586040					
Improper Check for Unusual or Exceptional	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580,	https://www.se.com/ww/en/download/docum	H-SCH-BMEP-171220/1397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conditions			Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	ent/SEVD-2020-343-08/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1398
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-BMEP-171220/1399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7543**		
modicon_m258					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Dec-20	5.2	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Modicon M258 Firmware (All versions prior to V5.0.4.11) and SoMachine/SoMachine Motion software (All versions), that could cause a buffer overflow when the length of a file transferred to the webserver is not verified. **CVE ID : CVE-2020-28220**	https://www.se.com/ww/en/download/document/SEVD-2020-343-09/	H-SCH-MODI-171220/1400
bmxnor0200h					
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP.	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	H-SCH-BMXN-171220/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7536		
bmxnoe0100					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	H-SCH-BMXN-171220/1402
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-BMXN-171220/1403
Improper Check for	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional	https://www.se.com/w	H-SCH-BMXN-171220/1404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unusual or Exceptional Conditions			Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	w/en/download/document/SEVD-2020-343-07/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXN-171220/1405
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-BMXN-171220/1406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**		
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXN-171220/1407
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-BMXN-171220/1408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sent to the controller over HTTP. **CVE ID : CVE-2020-7549**		
bmxnoe0110					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	H-SCH-BMXN-171220/1409
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-BMXN-171220/1410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	7.8	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP. **CVE ID : CVE-2020-7536**	https://www.se.com/ww/en/download/document/SEVD-2020-343-07/	H-SCH-BMXN-171220/1411
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXN-171220/1412
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy	https://www.se.com/ww/en/download/document/SEVD-	H-SCH-BMXN-171220/1413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	2020-343-04/	
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXN-171220/1414
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-BMXN-171220/1415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**		
bmxnoc0401					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	H-SCH-BMXN-171220/1416
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP.	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXN-171220/1417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7539		
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-BMXN-171220/1418
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-BMXN-171220/1419
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum	https://www.se.com/ww/en/download/document/SEVD-2020-343-	H-SCH-BMXN-171220/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	06/	
tsxp574634					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	H-SCH-TSXP-171220/1421
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-TSXP-171220/1422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-TSXP-171220/1423
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP.	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-TSXP-171220/1424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7539		
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-TSXP-171220/1425
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-TSXP-171220/1426
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon	https://www.se.com/ww/en/download/document/SEVD-2020-343-	H-SCH-TSXP-171220/1427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	08/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-TSXP-171220/1428
tsxp575634					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of	N/A	H-SCH-TSXP-171220/1429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-TSXP-171220/1430
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller.	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-TSXP-171220/1431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7537		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-TSXP-171220/1432
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-TSXP-171220/1433
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers	https://www.se.com/ww/en/download/document/SEVD-	H-SCH-TSXP-171220/1434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	2020-343-03/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-TSXP-171220/1435
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-TSXP-171220/1436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**		
tsxp576634					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	H-SCH-TSXP-171220/1437
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-TSXP-171220/1438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controller over HTTP. **CVE ID : CVE-2020-7535**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7537**	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-TSXP-171220/1439
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-TSXP-171220/1440
Missing Authenticati on for	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists	https://www.se.com/ww/en/down	H-SCH-TSXP-171220/1441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Function			in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	load/document/SEVD-2020-343-04/	
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-TSXP-171220/1442
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-08/	H-SCH-TSXP-171220/1443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller. **CVE ID : CVE-2020-7542**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-TSXP-171220/1444
tsxety4103					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted	N/A	H-SCH-TSXE-171220/1445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP requests. **CVE ID : CVE-2020-7533**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-TSXE-171220/1446
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-TSXE-171220/1447
Missing	11-Dec-20	7.5	A CWE-306: Missing	https://ww	H-SCH-TSXE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication for Critical Function			Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	w.se.com/ww/en/download/document/SEVD-2020-343-04/	171220/1448
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-TSXE-171220/1449
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-TSXE-171220/1450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**		
tsxety5103					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	H-SCH-TSXE-171220/1451
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-TSXE-171220/1452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-TSXE-171220/1453
Missing Authenticati on for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-TSXE-171220/1454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-TSXE-171220/1455
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-TSXE-171220/1456
140noc78000					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and	N/A	H-SCH-140N-171220/1457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-140N-171220/1458
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-140N-171220/1459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**		
Missing Authenticati on for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-04/	H-SCH-140N-171220/1460
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP.	https://ww w.se.com/w w/en/down load/docum ent/SEVD-2020-343-03/	H-SCH-140N-171220/1461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7541		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-140N-171220/1462
140noc77101					
N/A	01-Dec-20	7.5	A CWE-255: Credentials Management vulnerability exists in Web Server on Modicon M340, Modicon Quantum and ModiconPremium Legacy offers and their Communication Modules (see security notification for version information) which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests. **CVE ID : CVE-2020-7533**	N/A	H-SCH-140N-171220/1463
Improper Limitation of a Pathname	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path	https://www.se.com/ww/en/down	H-SCH-140N-171220/1464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**	load/document/SEVD-2020-343-05/	
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-140N-171220/1465
Missing Authentication for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-140N-171220/1466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**		
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-140N-171220/1467
140noc78100					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-20	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause	https://www.se.com/ww/en/download/document/SEVD-2020-343-05/	H-SCH-140N-171220/1468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure of information when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7535**		
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP. **CVE ID : CVE-2020-7539**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-140N-171220/1469
Missing Authenticati on for Critical Function	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	https://www.se.com/ww/en/download/document/SEVD-2020-343-04/	H-SCH-140N-171220/1470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Direct Request ('Forced Browsing')	11-Dec-20	5	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP. **CVE ID : CVE-2020-7541**	https://www.se.com/ww/en/download/document/SEVD-2020-343-03/	H-SCH-140N-171220/1471
Improper Check for Unusual or Exceptional Conditions	11-Dec-20	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP. **CVE ID : CVE-2020-7549**	https://www.se.com/ww/en/download/document/SEVD-2020-343-06/	H-SCH-140N-171220/1472
bmxnor200h					
Missing Authentication for Critical	11-Dec-20	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy	https://www.se.com/ww/en/download/document/SEVD-	H-SCH-BMXN-171220/1473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests. **CVE ID : CVE-2020-7540**	2020-343-04/	
acti9_smartlink_si_d					
Use of Insufficiently Random Values	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login. **CVE ID : CVE-2020-7548**	N/A	H-SCH-ACTI-171220/1474
acti9_smartlink_si_b					
Use of Insufficiently Random Values	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login. **CVE ID : CVE-2020-7548**	N/A	H-SCH-ACTI-171220/1475
acti9_powertag_link					
Use of Insufficiently Random	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in	N/A	H-SCH-ACTI-171220/1476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Values			Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login. **CVE ID : CVE-2020-7548**		
acti9_powertag_link_hd					
Use of Insufficiently Random Values	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login. **CVE ID : CVE-2020-7548**	N/A	H-SCH-ACTI-171220/1477
acti9_smartlink_el_b					
Use of Insufficiently Random Values	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login. **CVE ID : CVE-2020-7548**	N/A	H-SCH-ACTI-171220/1478
wiser_link					
Use of Insufficiently Random Values	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that	N/A	H-SCH-WISE-171220/1479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow unauthorized users to login. **CVE ID : CVE-2020-7548**		
wiser_energy					
Use of Insufficiently Random Values	01-Dec-20	7.5	A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login. **CVE ID : CVE-2020-7548**	N/A	H-SCH-WISE-171220/1480
Singtel					
askey_ap5100w-d171					
Weak Password Requirements	10-Dec-20	10	Askey AP5100W_Dual_SIG_1.01.097 and all prior versions use a weak password at the Operating System (rlx-linux) level. This allows an attacker to gain unauthorized access as an admin or root user to the device Operating System via Telnet or SSH. **CVE ID : CVE-2020-26201**	https://www.askey.com.tw/incident_report_notifications.html	H-SIN-ASKE-171220/1481
Wago					
750-352					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	H-WAG-750--171220/1482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
750-829					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	H-WAG-750--171220/1483
750-831					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	H-WAG-750--171220/1484
750-852					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	H-WAG-750--171220/1485
750-880					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	H-WAG-750--171220/1486
750-881					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x	https://cert.vde.com/en-	H-WAG-750--171220/1487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	us/advisories/vde-2020-042	
750-882					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	H-WAG-750--171220/1488
750-885					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	H-WAG-750--171220/1489
750-889					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	H-WAG-750--171220/1490
750-331					
N/A	10-Dec-20	5	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack. **CVE ID : CVE-2020-12516**	https://cert.vde.com/en-us/advisories/vde-2020-042	H-WAG-750--171220/1491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
westerndigital					
my_cloud_ex2_ultra					
N/A	01-Dec-20	7.5	On Western Digital My Cloud OS 5 devices before 5.06.115, the NAS Admin dashboard has an authentication bypass vulnerability that could allow an unauthenticated user to execute privileged commands on the device. **CVE ID : CVE-2020-28940**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1492
N/A	01-Dec-20	7.5	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.06.115. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to execute privileged commands on the device via a cookie. (In addition, an upload endpoint could then be used by an authenticated administrator to upload executable PHP scripts.) **CVE ID : CVE-2020-28970**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1493
Improper Input Validation	01-Dec-20	7.5	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.06.115. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to execute privileged commands on the device via a cookie, because of insufficient validation of URI paths. **CVE ID : CVE-2020-28971**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
my_cloud_ex4100					
N/A	01-Dec-20	7.5	On Western Digital My Cloud OS 5 devices before 5.06.115, the NAS Admin dashboard has an authentication bypass vulnerability that could allow an unauthenticated user to execute privileged commands on the device. **CVE ID : CVE-2020-28940**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1495
N/A	01-Dec-20	7.5	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.06.115. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to execute privileged commands on the device via a cookie. (In addition, an upload endpoint could then be used by an authenticated administrator to upload executable PHP scripts.) **CVE ID : CVE-2020-28970**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1496
Improper Input Validation	01-Dec-20	7.5	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.06.115. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to execute privileged commands on the device via a cookie, because of insufficient validation of URI paths. **CVE ID : CVE-2020-28971**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1497
my_cloud_pr2100					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Dec-20	7.5	On Western Digital My Cloud OS 5 devices before 5.06.115, the NAS Admin dashboard has an authentication bypass vulnerability that could allow an unauthenticated user to execute privileged commands on the device. **CVE ID : CVE-2020-28940**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1498
N/A	01-Dec-20	7.5	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.06.115. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to execute privileged commands on the device via a cookie. (In addition, an upload endpoint could then be used by an authenticated administrator to upload executable PHP scripts.) **CVE ID : CVE-2020-28970**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1499
Improper Input Validation	01-Dec-20	7.5	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.06.115. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to execute privileged commands on the device via a cookie, because of insufficient validation of URI paths. **CVE ID : CVE-2020-28971**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1500
my_cloud_pr4100					
N/A	01-Dec-20	7.5	On Western Digital My Cloud	https://ww	H-WES-MY_C-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OS 5 devices before 5.06.115, the NAS Admin dashboard has an authentication bypass vulnerability that could allow an unauthenticated user to execute privileged commands on the device. **CVE ID : CVE-2020-28940**	w.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	171220/1501
N/A	01-Dec-20	7.5	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.06.115. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to execute privileged commands on the device via a cookie. (In addition, an upload endpoint could then be used by an authenticated administrator to upload executable PHP scripts.) **CVE ID : CVE-2020-28970**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1502
Improper Input Validation	01-Dec-20	7.5	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.06.115. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to execute privileged commands on the device via a cookie, because of insufficient validation of URI paths. **CVE ID : CVE-2020-28971**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1503
my_cloud_mirror_gen_2					
N/A	01-Dec-20	7.5	On Western Digital My Cloud OS 5 devices before	https://www.westernd	H-WES-MY_C-171220/1504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.06.115, the NAS Admin dashboard has an authentication bypass vulnerability that could allow an unauthenticated user to execute privileged commands on the device. **CVE ID : CVE-2020-28940**	igital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	
N/A	01-Dec-20	7.5	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.06.115. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to execute privileged commands on the device via a cookie. (In addition, an upload endpoint could then be used by an authenticated administrator to upload executable PHP scripts.) **CVE ID : CVE-2020-28970**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1505
Improper Input Validation	01-Dec-20	7.5	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.06.115. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to execute privileged commands on the device via a cookie, because of insufficient validation of URI paths. **CVE ID : CVE-2020-28971**	https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115	H-WES-MY_C-171220/1506
ZTE					
zxv10_w908					
Improper Neutralizatio	01-Dec-20	7.5	A ZXELINK wireless controller has a SQL	N/A	H-ZTE-ZXV1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an SQL Command ('SQL Injection')			injection vulnerability. A remote attacker does not need to log in. By sending malicious SQL statements, because the device does not properly filter parameters, successful use can obtain management rights. This affects: ZXV10 W908 all versions before MIPS_A_1022IPV6R3T6P7Y20. **CVE ID : CVE-2020-6880**		171220/1507