Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
4mosan					
gcb_doctor					
Improper Authentication	19-Nov-21	10	4MOSAn GCB Doctor's login page has improper validation of Cookie, which allows an unauthenticated remote attacker to bypass authentication by code injection in cookie, and arbitrarily manipulate the system or interrupt services by upload and execution of arbitrary files. **CVE ID : CVE-2021-42338**	https://www.twcert.org.tw/tw/cp-132-5313-45bde-1.html	A-4MO-GCB_-061221/1
Acronis					
agent					
Insertion of Sensitive Information into Log File	29-Nov-21	5	Sensitive information could be logged. The following products are affected: Acronis Agent (Windows, Linux, macOS) before build 27147 **CVE ID : CVE-2021-34800**	https://security-advisory.acronis.com/advisories/SEC-3145	A-ACR-AGEN-061221/2
Uncontrolled Search Path Element	29-Nov-21	1.9	DLL hijacking could lead to denial of service. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27305, Acronis Cyber Protect Home Office (Windows) before build 39612	https://security-advisory.acronis.com/advisories/SEC-2508	A-ACR-AGEN-061221/3

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-44199		
cyber_protect					
Uncontrolled Search Path Element	29-Nov-21	4.4	DLL hijacking could lead to local privilege escalation. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035 **CVE ID : CVE-2021-44198**	https://security-advisory.acronis.com/advisories/SEC-2128	A-ACR-CYBE-061221/4
Uncontrolled Search Path Element	29-Nov-21	1.9	DLL hijacking could lead to denial of service. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27305, Acronis Cyber Protect Home Office (Windows) before build 39612 **CVE ID : CVE-2021-44199**	https://security-advisory.acronis.com/advisories/SEC-2508	A-ACR-CYBE-061221/5
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	Self cross-site scripting (XSS) was possible on devices page. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035 **CVE ID : CVE-2021-44200**	https://security-advisory.acronis.com/advisories/SEC-2803	A-ACR-CYBE-061221/6
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	4.3	Cross-site scripting (XSS) was possible in notification pop-ups. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035 **CVE ID : CVE-2021-44201**	https://security-advisory.acronis.com/advisories/SEC-3167	A-ACR-CYBE-061221/7
Improper Neutralizatio	29-Nov-21	3.5	Stored cross-site scripting (XSS) was possible in activity	https://security-	A-ACR-CYBE-061221/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			details. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035 **CVE ID : CVE-2021-44202**	advisory.acronis.com/advisories/SEC-3283	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	Stored cross-site scripting (XSS) was possible in protection plan details. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035 **CVE ID : CVE-2021-44203**	https://security-advisory.acronis.com/advisories/SEC-3294	A-ACR-CYBE-061221/9
cyber_protect_home_office					
Uncontrolled Search Path Element	29-Nov-21	1.9	DLL hijacking could lead to denial of service. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27305, Acronis Cyber Protect Home Office (Windows) before build 39612 **CVE ID : CVE-2021-44199**	https://security-advisory.acronis.com/advisories/SEC-2508	A-ACR-CYBE-061221/10
acurax					
floating_social_media_icon					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Nov-21	3.5	Authenticated Stored Cross-Site Scripting (XSS) vulnerability discovered in WordPress Floating Social Media Icon plugin (versions <= 4.3.5) Social Media Configuration form. Requires high role user like admin. **CVE ID : CVE-2021-36843**	https://wordpress.org/plugins/floating-social-media-icon/	A-ACU-FLOA-061221/11
Adobe					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
after_effects					
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious .m4a file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40751**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	A-ADO-AFTE-061221/12
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious .m4a file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40752**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	A-ADO-AFTE-061221/13
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SVG file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	A-ADO-AFTE-061221/14

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40753**		
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40754**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	A-ADO-AFTE-061221/15
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SGI file in the DoReadContinue function, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. **CVE ID : CVE-2021-40755**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	A-ADO-AFTE-061221/16
NULL Pointer Dereference	18-Nov-21	4.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	A-ADO-AFTE-061221/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application denial-of-service 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-2021-40756**		
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious MXF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40757**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	A-ADO-AFTE-061221/18
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40758**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	A-ADO-AFTE-061221/19
Access of Memory Location After End of	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure	https://helpx.adobe.com/security/products/after	A-ADO-AFTE-061221/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			handling of a malicious .m4a file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40759**	_effects/apsb21-79.html	
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious .m4a file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40760**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	A-ADO-AFTE-061221/21
NULL Pointer Dereference	18-Nov-21	4.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2021-40761**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	A-ADO-AFTE-061221/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
animate					
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe Animate version 21.0.9 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious .psd file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. **CVE ID : CVE-2021-40733**	https://helpx.adobe.com/security/products/animate/apsb21-105.html	A-ADO-ANIM-061221/23
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe Animate version 21.0.9 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious FLA file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. **CVE ID : CVE-2021-42266**	https://helpx.adobe.com/security/products/animate/apsb21-105.html	A-ADO-ANIM-061221/24
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Nov-21	9.3	Adobe Animate version 21.0.9 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious FLA file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. **CVE ID : CVE-2021-42267**	https://helpx.adobe.com/security/products/animate/apsb21-105.html	A-ADO-ANIM-061221/25
NULL Pointer	18-Nov-21	4.3	Adobe Animate version 21.0.9 (and earlier) is affected by a	https://helpx.adobe.com	A-ADO-ANIM-061221/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			Null pointer dereference vulnerability when parsing a specially crafted FLA file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2021-42268**	/security/products/animate/apsb21-105.html	
Use After Free	18-Nov-21	9.3	Adobe Animate version 21.0.9 (and earlier) are affected by a use-after-free vulnerability in the processing of a malformed FLA file 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-2021-42269**	https://helpx.adobe.com/security/products/animate/apsb21-105.html	A-ADO-ANIM-061221/27
Out-of-bounds Write	18-Nov-21	9.3	Adobe Animate version 21.0.9 (and earlier) are affected by an out-of-bounds write 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 BMP file. **CVE ID : CVE-2021-42270**	https://helpx.adobe.com/security/products/animate/apsb21-105.html	A-ADO-ANIM-061221/28
Out-of-bounds Write	18-Nov-21	9.3	Adobe Animate version 21.0.9 (and earlier) are affected by an out-of-bounds write	https://helpx.adobe.com/security/pr	A-ADO-ANIM-061221/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 BMP file. **CVE ID : CVE-2021-42271**	oducts/animate/apsb21-105.html	
Out-of-bounds Write	18-Nov-21	9.3	Adobe Animate version 21.0.9 (and earlier) are affected by an out-of-bounds write 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 GIF file. **CVE ID : CVE-2021-42272**	https://helpx.adobe.com/security/products/animate/apsb21-105.html	A-ADO-ANIM-061221/30
Out-of-bounds Write	18-Nov-21	9.3	Adobe Animate version 21.0.9 (and earlier) are affected by an out-of-bounds write 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 BMP file. **CVE ID : CVE-2021-42524**	https://helpx.adobe.com/security/products/animate/apsb21-105.html	A-ADO-ANIM-061221/31
Out-of-bounds Read	18-Nov-21	4.3	Acrobat Animate versions 21.0.9 (and earlier)is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this	https://helpx.adobe.com/security/products/animate/apsb21-105.html	A-ADO-ANIM-061221/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-42525**		
audition					
Out-of-bounds Read	19-Nov-21	4.3	Adobe Audition version 14.2 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose arbitrary memory information 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-2021-36003**	https://helpx.adobe.com/security/products/audition/apsb21-62.html	A-ADO-AUDI-061221/33
campaign					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Nov-21	5	Adobe Campaign version 21.2.1 (and earlier) is affected by a Path Traversal vulnerability that could lead to reading arbitrary server files. By leveraging an exposed XML file, an unauthenticated attacker can enumerate other files on the server. **CVE ID : CVE-2021-40745**	https://helpx.adobe.com/security/products/campaign/apsb21-52.html	A-ADO-CAMP-061221/34
creative_cloud_desktop_application					
N/A	18-Nov-21	3.5	Adobe Creative Cloud version 5.5 (and earlier) are affected by an Application denial of service vulnerability in the Creative Cloud Desktop	https://helpx.adobe.com/security/products/creative-	A-ADO-CREA-061221/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installer. An authenticated attacker could leverage this vulnerability to achieve denial of service in the context of the user. User interaction is required before product installation to abuse this vulnerability. **CVE ID : CVE-2021-43017**	cloud/apsb21-111.html	
Improper Access Control	23-Nov-21	9.3	Adobe Creative Cloud version 5.5 (and earlier) are affected by a privilege escalation vulnerability in the resources leveraged by the Setup.exe service. An unauthenticated attacker could leverage this vulnerability to remove files and escalate privileges under the context of SYSTEM . An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability on the product installer. User interaction is required before product installation to abuse this vulnerability. **CVE ID : CVE-2021-43019**	https://helpx.adobe.com/security/products/creative-cloud/apsb21-111.html, https://www.zerodayinitiative.com/advisories/ZDI-21-1333/	A-ADO-CREA-061221/36
experience_manager					
Incorrect Authorization	16-Nov-21	5	Adobe Experience Manager version 6.5.9.0 (and earlier) are affected by an improper access control vulnerability that leads to a security feature bypass. By manipulating referer headers, an unauthenticated attacker could gain access to arbitrary	https://helpx.adobe.com/security/products/experience-manager/apsb21-82.html	A-ADO-EXPE-061221/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pages that they are not authorized to access. **CVE ID : CVE-2021-42725**		
experience_manager_cloud_service					
Incorrect Authorization	16-Nov-21	5	Adobe Experience Manager version 6.5.9.0 (and earlier) are affected by an improper access control vulnerability that leads to a security feature bypass. By manipulating referer headers, an unauthenticated attacker could gain access to arbitrary pages that they are not authorized to access. **CVE ID : CVE-2021-42725**	https://helpx.adobe.com/security/products/experience-manager/apsb21-82.html	A-ADO-EXPE-061221/38
incopy					
Access of Memory Location After End of Buffer	22-Nov-21	9.3	Adobe InCopy version 16.4 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious GIF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-43015**	https://helpx.adobe.com/security/products/incopy/apsb21-110.html	A-ADO-INCO-061221/39
NULL Pointer Dereference	22-Nov-21	4.3	Adobe InCopy version 16.4 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this	https://helpx.adobe.com/security/products/incopy/apsb21-110.html	A-ADO-INCO-061221/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to achieve an application denial-of-service 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-2021-43016**		
indesign					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Nov-21	9.3	Adobe InDesign versions 16.4 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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-2021-42731**	https://helpx.adobe.com/security/products/indesign/apsb21-107.html	A-ADO-INDE-061221/41
media_encoder					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	9.3	Adobe Media Encoder version 15.4 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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 M4A file. **CVE ID : CVE-2021-42721**	https://helpx.adobe.com/security/products/media-encoder/apsb21-70.html	A-ADO-MEDI-061221/42

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access of Memory Location After End of Buffer	16-Nov-21	9.3	Adobe Media Encoder version 15.4 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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 M4A file. **CVE ID : CVE-2021-42726**	https://helpx.adobe.com/security/products/media-encoder/apsb21-70.html	A-ADO-MEDI-061221/43
Access of Memory Location After End of Buffer	16-Nov-21	9.3	Adobe Media Encoder version 15.4.1 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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-2021-43013**	https://helpx.adobe.com/security/products/media-encoder/apsb21-99.html	A-ADO-MEDI-061221/44
prelude					
Access of Memory Location After End of Buffer	22-Nov-21	6.8	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious M4A file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	A-ADO-PREL-061221/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40770**		
Access of Memory Location After End of Buffer	22-Nov-21	6.8	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40771**	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	A-ADO-PREL-061221/46
Access of Memory Location After End of Buffer	22-Nov-21	6.8	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious M4A file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40772**	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	A-ADO-PREL-061221/47
NULL Pointer Dereference	22-Nov-21	4.3	Adobe Prelude version 10.1 (and earlier) is affected by a null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	A-ADO-PREL-061221/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to achieve an application denial-of-service 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-2021-40773**		
NULL Pointer Dereference	22-Nov-21	4.3	Adobe Prelude version 10.1 (and earlier) is affected by a null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2021-40774**	https://help x.adobe.com /security/pr oducts/prel ude/apsb21-96.html	A-ADO-PREL-061221/49
Access of Memory Location After End of Buffer	22-Nov-21	6.8	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SVG file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40775**	https://help x.adobe.com /security/pr oducts/prel ude/apsb21-96.html	A-ADO-PREL-061221/50
Improper Input	22-Nov-21	6.8	Adobe Prelude version 10.1 (and earlier) is affected by an	https://help x.adobe.com	A-ADO-PREL-061221/51

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			improper input validation vulnerability in the XDCAMSAM directory. An unauthenticated attacker could leverage this vulnerability to execute arbitrary code 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-2021-42733**	/security/products/prelude/apsb21-96.html	
Access of Memory Location After End of Buffer	22-Nov-21	6.8	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-42737**	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	A-ADO-PREL-061221/52
Access of Memory Location After End of Buffer	22-Nov-21	9.3	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious MXF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	A-ADO-PREL-061221/53

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-42738		
Access of Memory Location After End of Buffer	16-Nov-21	9.3	Adobe Prelude version 10.1 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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 M4A file. **CVE ID : CVE-2021-43011**	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	A-ADO-PREL-061221/54
Access of Memory Location After End of Buffer	16-Nov-21	9.3	Adobe Prelude version 10.1 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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 M4A file. **CVE ID : CVE-2021-43012**	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	A-ADO-PREL-061221/55
premiere_pro					
Access of Memory Location After End of Buffer	16-Nov-21	9.3	Adobe Premiere Pro version 15.4 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current	https://helpx.adobe.com/security/products/premiere_pro/apsb21-67.html	A-ADO-PREM-061221/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user. Exploitation of this issue requires user interaction in that a victim must open a malicious M4A file. **CVE ID : CVE-2021-42723**		
robohelp_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Nov-21	6.8	Acrobat RoboHelp Server versions 2020.0.1 (and earlier) are affected by a Path traversal vulnerability. The authenticated attacker can upload arbitrary files outside of the intended directory to cause remote code execution with privileges of user running Tomcat. Exploitation of this issue requires user interaction in that a victim must navigate to a planted file on the server. **CVE ID : CVE-2021-42727**	https://helpx.adobe.com/security/products/robohelp-server/apsb21-87.html	A-ADO-ROBO-061221/57
advanced_access_manager_project					
advanced_access_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	3.5	The Advanced Access Manager WordPress plugin before 6.8.0 does not escape some of its settings when outputting them, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24830**	https://plugins.trac.wordpress.org/changeset/2616161/	A-ADV-ADVA-061221/58
advanced_forms_project					
advanced_forms					
Authorizatio	23-Nov-21	6.5	Insecure Direct Object	https://gith	A-ADV-ADVA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n Bypass Through User-Controlled Key			Reference in edit function of Advanced Forms (Free & Pro) before 1.6.9 allows authenticated remote attacker to change arbitrary user's email address and request for reset password, which could lead to take over of WordPress's administrator account. To exploit this vulnerability, an attacker must register to obtain a valid WordPress's user and use such user to authenticate with WordPress in order to exploit the vulnerable edit function. **CVE ID : CVE-2021-24892**	ub.com/advancedforms/advanced-forms/commit/2ce3ab6985c3a909eefb01c562995bc6a994d3a2	061221/59
aifu					
cashier_accounting_management_system					
Improper Authorization	16-Nov-21	4	The permission control of AIFU cashier management salary query function can be bypassed, thus after obtaining general user's permission, the remote attacker can access account information except passwords by crafting URL parameters. **CVE ID : CVE-2021-42337**	N/A	A-AIF-CASH-061221/60
aimstack					
aim					
Improper Limitation of a Pathname to a Restricted Directory ('Path	23-Nov-21	5	Aim is an open-source, self-hosted machine learning experiment tracking tool. Versions of Aim prior to 3.1.0 are vulnerable to a path traversal attack. By manipulating variables that	https://github.com/aimhubio/aim/security/advisories/GHSA-8phj-f9w2-cjcc,	A-AIM-AIM-061221/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			reference files with â€œdot-dot-slash (../)â€? sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. The vulnerability issue is resolved in Aim v3.1.0. **CVE ID : CVE-2021-43775**	https://github.com/aimhubio/aim/pull/1003, https://github.com/aimhubio/aim/blob/0b99c6ca08e0ba7e7011453a2f68033e9b1d1bce/aim/web/api/views.py#L9-L16	
alfasado					
powercms					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Nov-21	7.5	PowerCMS XMLRPC API of PowerCMS 5.19 and earlier, PowerCMS 4.49 and earlier, PowerCMS 3.295 and earlier, and PowerCMS 2 Series (End-of-Life, EOL) allows a remote attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20850**	https://www.powercms.jp/news/release-patch-xmlrpc-api-202110.html	A-ALF-POWE-061221/62
algolia					
algoliasearch-helper					
Improperly Controlled Modification of Dynamically-Determined Object Attributes	19-Nov-21	6.8	The package algoliasearch-helper before 3.6.2 are vulnerable to Prototype Pollution due to use of the merge function in src/SearchParameters/index.jsSearchParameters._parseNumbers without any protection against prototype properties. Note that this vulnerability is only exploitable if the	https://github.com/algolia/algoliasearch-helper-js/commit/4ff542b70b92a6b81cce8b9255700b0bc0817edd	A-ALG-ALGO-061221/63

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			implementation allows users to define arbitrary search patterns. **CVE ID : CVE-2021-23433**		
Apache					
apisix					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Nov-21	5	The uri-block plugin in Apache APISIX before 2.10.2 uses $request_uri without verification. The $request_uri is the full original request URI without normalization. This makes it possible to construct a URI to bypass the block list on some occasions. For instance, when the block list contains "^/internal/", a URI like `//internal/` can be used to bypass it. Some other plugins also have the same issue. And it may affect the developer's custom plugin. **CVE ID : CVE-2021-43557**	https://lists.apache.org/thread/18jyd458ptocr31rnkjs71w4h366mv7h	A-APA-APIS-061221/64
jspwiki					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Nov-21	4.3	A carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the Denounce plugin, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Apache JSPWiki users should upgrade to 2.11.0 or later. **CVE ID : CVE-2021-40369**	https://lists.apache.org/thread/r2j00nrnpjgcmoxvlv3pgfoq9kzrcsfh, https://jspwiki-wiki.apache.org/Wiki.jsp?page=CVE-2021-40369	A-APA-JSPW-061221/65
Incorrect	24-Nov-21	6.4	Remote attackers may delete	https://jspw	A-APA-JSPW-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Default Permissions			arbitrary files in a system hosting a JSPWiki instance, versions up to 2.11.0.M8, by using a carefuly crafted http request on logout, given that those files are reachable to the user running the JSPWiki instance. Apache JSPWiki users should upgrade to 2.11.0 or later. **CVE ID : CVE-2021-44140**	iki-wiki.apache.org/Wiki.jsp?page=CVE-2021-44140, https://lists.apache.org/thread/5qglpjdhvobppx7j550lf1sk28f6011t	061221/66
ozone					
Improper Check for Dropped Privileges	19-Nov-21	7.5	In Apache Ozone versions prior to 1.2.0, Initially generated block tokens are persisted to the metadata database and can be retrieved with authenticated users with permission to the key. Authenticated users may use them even after access is revoked. **CVE ID : CVE-2021-36372**	https://mail-archives.apache.org/mod_mbox/ozone-dev/202111.mbox/%3C5029c1ac-4685-8492-e3cb-ab48c5c370cf%40apache.org%3E	A-APA-OZON-061221/67
Exposure of Resource to Wrong Sphere	19-Nov-21	6.4	In Apache Ozone versions prior to 1.2.0, Various internal server-to-server RPC endpoints are available for connections, making it possible for an attacker to download raw data from Datanode and Ozone manager and modify Ratis replication configuration. **CVE ID : CVE-2021-39231**	https://mail-archives.apache.org/mod_mbox/ozone-dev/202111.mbox/%3C110cd117-75ed-364b-cd38-3effd20f2183%40apache	A-APA-OZON-061221/68

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org%3E	
Incorrect Authorization	19-Nov-21	6.5	In Apache Ozone versions prior to 1.2.0, certain admin related SCM commands can be executed by any authenticated users, not just by admins. **CVE ID : CVE-2021-39232**	https://mail-archives.apache.org/mod_mbox/ozone-dev/202111.mbox/%3C3c30a7f2-13a4-345e-6c8a-c23a2b937041%40apache.org%3E	A-APA-OZON-061221/69
Incorrect Authorization	19-Nov-21	6.4	In Apache Ozone versions prior to 1.2.0, Container related Datanode requests of Ozone Datanode were not properly authorized and can be called by any client. **CVE ID : CVE-2021-39233**	https://mail-archives.apache.org/mod_mbox/ozone-dev/202111.mbox/%3C394a9a73-44dd-b5db-84d8-607c3226eb00%40apache.org%3E	A-APA-OZON-061221/70
Incorrect Authorization	19-Nov-21	4.9	In Apache Ozone versions prior to 1.2.0, Authenticated users knowing the ID of an existing block can craft specific request allowing access those blocks, bypassing other security checks like ACL. **CVE ID : CVE-2021-39234**	https://mail-archives.apache.org/mod_mbox/ozone-dev/202111.mbox/%3C97d65498-7f8c-366f-1bea-	A-APA-OZON-061221/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				5a74b6378f0d%40apache.org%3E	
Incorrect Permission Assignment for Critical Resource	19-Nov-21	4	In Apache Ozone before 1.2.0, Ozone Datanode doesn't check the access mode parameter of the block token. Authenticated users with valid READ block token can do any write operation on the same block. **CVE ID : CVE-2021-39235**	https://mail-archives.apache.org/mod_mbox/ozone-dev/202111.mbox/%3C93f88246-4320-7423-0dac-ec7a07f47455%40apache.org%3E	A-APA-OZON-061221/72
Improper Authentication	19-Nov-21	6.5	In Apache Ozone before 1.2.0, Authenticated users with valid Ozone S3 credentials can create specific OM requests, impersonating any other user. **CVE ID : CVE-2021-39236**	https://mail-archives.apache.org/mod_mbox/ozone-dev/202111.mbox/%3C0fd74baa-88a0-39a2-8f3a-b982acb25d5a%40apache.org%3E	A-APA-OZON-061221/73
Exposure of Resource to Wrong Sphere	19-Nov-21	5	In Apache Ozone before 1.2.0, Recon HTTP endpoints provide access to OM, SCM and Datanode metadata. Due to a bug, any unauthenticated user can access the data from these endpoints. **CVE ID : CVE-2021-41532**	https://mail-archives.apache.org/mod_mbox/ozone-dev/202111.mbox/%3Ce0bc6598-	A-APA-OZON-061221/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				9669-b897-fc28-de8a896e36aa%40apache.org%3E	
shenyu					
Improper Authentication	16-Nov-21	7.5	A flaw was found in Apache ShenYu Admin. The incorrect use of JWT in ShenyuAdminBootstrap allows an attacker to bypass authentication. This issue affected Apache ShenYu 2.3.0 and 2.4.0 **CVE ID : CVE-2021-37580**	https://lists.apache.org/thread/o15j25qwtpcw62k48xw1tnv48skh3zgb	A-APA-SHEN-061221/75
superset					
Improper Encoding or Escaping of Output	17-Nov-21	4	Improper output neutralization for Logs. A specific Apache Superset HTTP endpoint allowed for an authenticated user to forge log entries or inject malicious content into logs. **CVE ID : CVE-2021-42250**	https://lists.apache.org/thread/53lkszw6d3tybp5t99nvgcj538b9trw9	A-APA-SUPE-061221/76
arangodb					
arangodb					
Insufficient Session Expiration	16-Nov-21	6	In ArangoDB, versions v3.7.6 through v3.8.3 are vulnerable to Insufficient Session Expiration. When a user's password is changed by the administrator, the session isn't invalidated, allowing a malicious user to still be logged in and perform arbitrary actions within the system. **CVE ID : CVE-2021-25940**	https://github.com/arangodb/arangodb/commit/e9c6ee9dcca7b9b4fbcd02a0b323d205bee838d3	A-ARA-ARAN-061221/77

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
awesomesupport					
awesome_support_wordpress_helpdesk_\\&_support					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Nov-21	3.5	Multiple Authenticated Reflected Cross-Site Scripting (XSS) vulnerabilities in WordPress Awesome Support plugin (versions <= 6.0.6), vulnerable parameters (&id, &assignee). **CVE ID : CVE-2021-36919**	https://wordpress.org/plugins/awesome-support/#developers	A-AWE-AWES-061221/78
backupbliss					
backup_migration					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Nov-21	3.5	Authenticated Persistent Cross-Site Scripting (XSS) vulnerability discovered in WordPress Backup Migration plugin <= 1.1.5 versions. **CVE ID : CVE-2021-36884**	https://wordpress.org/plugins/backup-backup/#developers, https://patchstack.com/database/vulnerability/backup-backup/wordpress-backup-migration-plugin-1-1-5-authenticated-persistent-cross-site-scripting-xss-vulnerability	A-BAC-BACK-061221/79
Bandisoft					
ark_library					
Integer	26-Nov-21	6.8	ARK library allows attackers	N/A	A-BAN-ARK_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			to execute remote code via the parameter(path value) of Ark_NormalizeAndDupPAthNameW function because of an integer overflow. **CVE ID : CVE-2021-26615**		061221/80
Bannersky					
bsk_pdf_manager					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Nov-21	6.5	The BSK PDF Manager WordPress plugin before 3.1.2 does not validate and escape the orderby and order parameters before using them in a SQL statement, leading to a SQL injection issue **CVE ID : CVE-2021-24860**	N/A	A-BAN-BSK_-061221/81
Basercms					
basercms					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Nov-21	9	There is a Potential Zip Slip Vulnerability and OS Command Injection Vulnerability on the management system of baserCMS. Users with permissions to upload files may upload crafted zip files which may execute arbitrary commands on the host operating system. This is a vulnerability that needs to be addressed when the management system is used by an unspecified number of users. If you are eligible, please update to the new version as soon as possible. **CVE ID : CVE-2021-41243**	https://github.com/baserproject/basercms/security/advisories/GHSA-7rpc-9m88-cf9w, https://github.com/baserproject/basercms/commit/9088b99c329d1faff3a2f1269f37b9a9d8d5f6ff	A-BAS-BASE-061221/82

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Nov-21	9	BaserCMS is an open source content management system with a focus on Japanese language support. In affected versions users with upload privilege may upload crafted zip files capable of path traversal on the host operating system. This is a vulnerability that needs to be addressed when the management system is used by an unspecified number of users. If you are eligible, please update to the new version as soon as possible. **CVE ID : CVE-2021-41279**	https://github.com/baserproject/basercms/security/advisories/GHSA-4x2f-54wr-4hjg, https://github.com/baserproject/basercms/commit/d8ab0a81a7bce35cc95ff7dff851a7e87a084336	A-BAS-BASE-061221/83
beyondtrust					
privilege_management_for_windows					
Exposure of Resource to Wrong Sphere	19-Nov-21	7.2	BeyondTrust Privilege Management prior to version 21.6 creates a Temporary File in a Directory with Insecure Permissions. **CVE ID : CVE-2021-42254**	N/A	A-BEY-PRIV-061221/84
Bitdefender					
endpoint_security_tools					
Server-Side Request Forgery (SSRF)	24-Nov-21	5	A Server-Side Request Forgery (SSRF) vulnerability in the EPPUpdateService component of Bitdefender Endpoint Security Tools allows an attacker to proxy requests to the relay server. This issue affects: Bitdefender Endpoint Security Tools versions prior to 6.6.27.390; versions prior to 7.1.2.33.	N/A	A-BIT-ENDP-061221/85

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bitdefender GravityZone 6.24.1-1. **CVE ID : CVE-2021-3552**		
Server-Side Request Forgery (SSRF)	24-Nov-21	5	A Server-Side Request Forgery (SSRF) vulnerability in the EPPUpdateService of Bitdefender Endpoint Security Tools allows an attacker to use the Endpoint Protection relay as a proxy for any remote host. This issue affects: Bitdefender Endpoint Security Tools versions prior to 6.6.27.390; versions prior to 7.1.2.33. Bitdefender Unified Endpoint for Linux versions prior to 6.2.21.160. Bitdefender GravityZone versions prior to 6.24.1-1. **CVE ID : CVE-2021-3553**	https://www.bitdefender.com/support/security-advisories/server-side-request-forgery-in-eppupdateservice-remote-config-file-va-9825/	A-BIT-ENDP-061221/86
gravityzone					
Server-Side Request Forgery (SSRF)	24-Nov-21	5	A Server-Side Request Forgery (SSRF) vulnerability in the EPPUpdateService component of Bitdefender Endpoint Security Tools allows an attacker to proxy requests to the relay server. This issue affects: Bitdefender Endpoint Security Tools versions prior to 6.6.27.390; versions prior to 7.1.2.33. Bitdefender GravityZone 6.24.1-1. **CVE ID : CVE-2021-3552**	N/A	A-BIT-GRAV-061221/87
Server-Side Request Forgery (SSRF)	24-Nov-21	5	A Server-Side Request Forgery (SSRF) vulnerability in the EPPUpdateService of Bitdefender Endpoint	https://www.bitdefender.com/support/security-	A-BIT-GRAV-061221/88

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Security Tools allows an attacker to use the Endpoint Protection relay as a proxy for any remote host. This issue affects: Bitdefender Endpoint Security Tools versions prior to 6.6.27.390; versions prior to 7.1.2.33. Bitdefender Unified Endpoint for Linux versions prior to 6.2.21.160. Bitdefender GravityZone versions prior to 6.24.1-1. **CVE ID : CVE-2021-3553**	advisories/server-side-request-forgery-in-eppupdateservice-remote-config-file-va-9825/	
brainstormforce					
starter_templates					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	3.5	On sites that also had the Elementor plugin for WordPress installed, it was possible for users with the edit_posts capability, which includes Contributor-level users, to import blocks onto any page using the astra-page-elementor-batch-process AJAX action. An attacker could craft and host a block containing malicious JavaScript on a server they controlled, and then use it to overwrite any post or page by sending an AJAX request with the action set to astra-page-elementor-batch-process and the url parameter pointed to their remotely-hosted malicious block, as well as an id parameter containing the post or page to overwrite. Any post or page that had been built with Elementor,	N/A	A-BRA-STAR-061221/89

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			including published pages, could be overwritten by the imported block, and the malicious JavaScript in the imported block would then be executed in the browser of any visitors to that page. **CVE ID : CVE-2021-42360**		
bulk_datetime_change_project					
bulk_datetime_change					
Missing Authorization	29-Nov-21	5.5	The Bulk Datetime Change WordPress plugin before 1.12 does not enforce capability checks which allows users with Contributor roles to 1) list private post titles of other users and 2) change the posted date of other users' posts. **CVE ID : CVE-2021-24842**	https://plugins.trac.wordpress.org/changeset/2618982	A-BUL-BULK-061221/90
businessdnasolutions					
topease					
Incorrect Permission Assignment for Critical Resource	30-Nov-21	6.4	Missing HTTPOnly flag in Web Applications operating on Business-DNA Solutions GmbHâ€™s TopEaseÂ® Platform Version <= 7.1.27 allows an unauthenticated remote attacker to escalate privileges from unauthenticated to authenticated user via stealing and injecting the session- independent and static cookie UID. **CVE ID : CVE-2021-42115**	https://confluence.topease.ch/confluence/display/DOC/Release+Notes	A-BUS-TOPE-061221/91
Exposure of Resource to	30-Nov-21	4	Incorrect Access Control in Web Applications operating	https://confluence.topeas	A-BUS-TOPE-061221/92

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			on Business-DNA Solutions GmbHâ€™s TopEaseÂ® Platform Version <= 7.1.27 allows an authenticated remote attacker to view the Shape Editor and Settings, which are functionality for higher privileged users, via identifying said components in the front-end source code or other means. **CVE ID : CVE-2021-42116**	e.ch/confluence/display/DOC/Release+Notes	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	30-Nov-21	4	Insufficient Input Validation in Web Applications operating on Business-DNA Solutions GmbH's TopEase® Platform Version <= 7.1.27 allows an authenticated remote attacker with Object Modification privileges to insert arbitrary HTML without code execution. **CVE ID : CVE-2021-42117**	https://confluence.topease.ch/confluence/display/DOC/Release+Notes	A-BUS-TOPE-061221/93
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Nov-21	3.5	Persistent Cross Site Scripting in Web Applications operating on Business-DNA Solutions GmbHâ€™s TopEaseÂ® Platform Version <= 7.1.27 via the Structure Component allows an authenticated remote attacker with Object Modification privileges to inject arbitrary HTML and JavaScript code in an object attribute, which is then rendered in the Structure Component, to alter the intended functionality and steal cookies, the latter allowing for account takeover.	https://confluence.topease.ch/confluence/display/DOC/Release+Notes	A-BUS-TOPE-061221/94

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-42118		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Nov-21	3.5	Persistent Cross Site Scripting in Web Applications operating on Business-DNA Solutions GmbHâ€™s TopEaseÂ® Platform Version <= 7.1.27 via the Search Functionality allows authenticated users with Object Modification privileges to inject arbitrary HTML and JavaScript in object attributes, which is then rendered in the Search Functionality, to alter the intended functionality and steal cookies, the latter allowing for account takeover. **CVE ID : CVE-2021-42119**	https://confluence.topease.ch/confluence/display/DOC/Release+Notes	A-BUS-TOPE-061221/95
Uncontrolled Resource Consumption	30-Nov-21	4	Insufficient Input Validation in Web Applications operating on Business-DNA Solutions GmbHâ€™s TopEaseÂ® Platform Version <= 7.1.27 on all object attributes allows an authenticated remote attacker with Object Modification privileges to insert arbitrarily long strings, eventually leading to exhaustion of the underlying resource. **CVE ID : CVE-2021-42120**	https://confluence.topease.ch/confluence/display/DOC/Release+Notes	A-BUS-TOPE-061221/96
Improper Input Validation	30-Nov-21	4	Insufficient Input Validation in Web Applications operating on Business-DNA Solutions GmbHâ€™s TopEaseÂ® Platform Version <= 7.1.27 on an objectâ€™s date attribute(s) allows an authenticated remote attacker	https://confluence.topease.ch/confluence/display/DOC/Release+Notes	A-BUS-TOPE-061221/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with Object Modification privileges to insert an unexpected format into date fields, which leads to breaking the object page that the date field is present. **CVE ID : CVE-2021-42121**		
Improper Input Validation	30-Nov-21	4	Insufficient Input Validation in Web Applications operating on Business-DNA Solutions GmbHâ€™s TopEaseÂ® Platform Version <= 7.1.27 on an objectâ€™s attributes with numeric format allows an authenticated remote attacker with Object Modification privileges to insert an unexpected format, which makes the affected attribute non-editable. **CVE ID : CVE-2021-42122**	https://confluence.topease.ch/confluence/display/DOC/Release+Notes	A-BUS-TOPE-061221/98
Unrestricted Upload of File with Dangerous Type	30-Nov-21	6.5	Unrestricted File Upload in Web Applications operating on Business-DNA Solutions GmbHâ€™s TopEaseÂ® Platform Version <= 7.1.27 in the File Upload Functions allows an authenticated remote attacker with Upload privileges to upload files with any file type, enabling client-side attacks. **CVE ID : CVE-2021-42123**	https://confluence.topease.ch/confluence/display/DOC/Release+Notes	A-BUS-TOPE-061221/99
Improper Restriction of Excessive Authentication Attempts	30-Nov-21	7.5	Missing Rate Limiting in Web Applications operating on Business-DNA Solutions GmbHâ€™s TopEaseÂ® Platform Version <= 7.1.27 on the Login Form allows an	https://confluence.topease.ch/confluence/display/DOC/Release+Notes	A-BUS-TOPE-061221/100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to perform multiple login attempts, which facilitates gaining privileges. **CVE ID : CVE-2021-42544**		
c-ares_project					
c-ares					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**	https://c-ares.haxx.se/adv_20210810.html	A-C-A-C-AR-061221/101
calibre-web_project					
calibre-web					
Cross-Site Request Forgery (CSRF)	16-Nov-21	6.8	In Calibre-web, versions 0.6.0 to 0.6.13 are vulnerable to Cross-Site Request Forgery (CSRF). By luring an authenticated user to click on a link, an attacker can create a new user role with admin privileges and attacker-controlled credentials, allowing them to take over the application. **CVE ID : CVE-2021-25965**	https://github.com/janeczku/calibre-web/commit/50919d47212066c75f03ee7a5332ecf2d584b98e	A-CAL-CALI-061221/102
Canonical					
accountsservice					
Release of	17-Nov-21	7.2	Ubuntu-specific modifications	https://ubu	A-CAN-ACCO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Invalid Pointer or Reference			to accountsservice (in patch file debian/patches/0010-set-language.patch) caused the fallback_locale variable, pointing to static storage, to be freed, in the user_change_language_authorized_cb function. This is reachable via the SetLanguage dbus function. This is fixed in versions 0.6.55-0ubuntu12~20.04.5, 0.6.55-0ubuntu13.3, 0.6.55-0ubuntu14.1. **CVE ID : CVE-2021-3939**	ntu.com/security/notices/USN-5149-1	061221/103
Cisco					
common_services_platform_collector					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Nov-21	4	A vulnerability in the configuration dashboard of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to submit a SQL query through the CSPC configuration dashboard. This vulnerability is due to insufficient input validation of uploaded files. An attacker could exploit this vulnerability by uploading a file containing a SQL query to the configuration dashboard. A successful exploit could allow the attacker to read restricted information from the CSPC SQL database. **CVE ID : CVE-2021-40129**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-CSPC-SQLI-unVPTn5	A-CIS-COMM-061221/104
Improper Authenticati	19-Nov-21	4	A vulnerability in the web application of Cisco Common	https://tools.cisco.com/s	A-CIS-COMM-061221/105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			Services Platform Collector (CSPC) could allow an authenticated, remote attacker to specify non-log files as sources for syslog reporting. This vulnerability is due to improper restriction of the syslog configuration. An attacker could exploit this vulnerability by configuring non-log files as sources for syslog reporting through the web application. A successful exploit could allow the attacker to read non-log files on the CSPC. **CVE ID : CVE-2021-40130**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-CSPC-ILR-8qmW8y8X	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Nov-21	3.5	A vulnerability in the web-based management interface of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input that is processed by the web-based management interface. An attacker could exploit this vulnerability by adding malicious code to the configuration by using the web-based management interface. A successful exploit could allow the attacker to execute arbitrary code in the context of the interface or access sensitive, browser-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-CSPC-XSS-KjrNbM3p	A-CIS-COMM-061221/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			based information. **CVE ID : CVE-2021-40131**		
Ckeditor					
ckeditor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	3.5	CKEditor4 is an open source WYSIWYG HTML editor. In affected versions a vulnerability has been discovered in the Advanced Content Filter (ACF) module and may affect all plugins used by CKEditor 4. The vulnerability allowed to inject malformed HTML bypassing content sanitization, which could result in executing JavaScript code. It affects all users using the CKEditor 4 at version < 4.17.0. The problem has been recognized and patched. The fix will be available in version 4.17.0. **CVE ID : CVE-2021-41164**	https://github.com/ckeditor/ckeditor4/security/advisories/GHSA-pvmx-g8h5-cprj, https://github.com/ckeditor/ckeditor4/blob/major/CHANGES.md#ckeditor-417, https://www.drupal.org/sa-core-2021-011	A-CKE-CKED-061221/107
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	3.5	CKEditor4 is an open source WYSIWYG HTML editor. In affected version a vulnerability has been discovered in the core HTML processing module and may affect all plugins used by CKEditor 4. The vulnerability allowed to inject malformed comments HTML bypassing content sanitization, which could result in executing JavaScript code. It affects all users using the CKEditor 4 at version < 4.17.0. The problem has been recognized and	https://github.com/ckeditor/ckeditor4/security/advisories/GHSA-7h26-63m7-qhf2, https://www.drupal.org/sa-core-2021-011	A-CKE-CKED-061221/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			patched. The fix will be available in version 4.17.0. **CVE ID : CVE-2021-41165**		
claris					
filemaker_pro					
Improper Restriction of XML External Entity Reference	22-Nov-21	4.3	An XML External Entity issue in Claris FileMaker Pro and Server (including WebDirect) before 19.4.1 allows a remote attacker to disclose local files via a crafted XML/Excel document and perform server-side request forgery attacks. **CVE ID : CVE-2021-44147**	https://support.claris.com/s/answerview?anum=000035751	A-CLA-FILE-061221/109
filemaker_server					
Improper Restriction of XML External Entity Reference	22-Nov-21	4.3	An XML External Entity issue in Claris FileMaker Pro and Server (including WebDirect) before 19.4.1 allows a remote attacker to disclose local files via a crafted XML/Excel document and perform server-side request forgery attacks. **CVE ID : CVE-2021-44147**	https://support.claris.com/s/answerview?anum=000035751	A-CLA-FILE-061221/110
Codepeople					
contact_form_email					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	2.1	The Contact Form Email WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and escaping via the name parameter found in the ~/trunk/cp-admin-int-list.inc.php file which allowed	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&repo name=&old=2628041%40contact-	A-COD-CONT-061221/111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.3.24. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. **CVE ID : CVE-2021-42361**	form-to-email&new=2628041%40contact-form-to-email&sfp_email=&sfph_mail=	
concretecms					
concrete_cms					
Authorization Bypass Through User-Controlled Key	19-Nov-21	5	Unauthorized individuals could view password protected files using view_inline in Concrete CMS (previously concrete 5) prior to version 8.5.7. Concrete CMS now checks to see if a file has a password in view_inline and, if it does, the file is not rendered.For version 8.5.6, the following mitigations were put in place a. restricting file types for view_inline to images only b. putting a warning in the file manager to advise users.Credit for discovery: "Solar Security Research Team"Concrete CMS security team CVSS scoring is 5.3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:NThis fix is also in Concrete version 9.0.0 **CVE ID : CVE-2021-22951**	https://documentation.concretecms.org/developers/introduction/version-history/857-release-notes	A-CON-CONC-061221/112
Improper Privilege Management	19-Nov-21	6.5	Privilege escalation from Editor to Admin using Groups in Concrete CMS versions	https://documentation.concretecms.or	A-CON-CONC-061221/113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.5.6 and below. If a group is granted "view" permissions on the bulkupdate page, then users in that group can escalate to being an administrator with a specially crafted curl. Fixed by adding a check for group permissions before allowing a group to be moved. Concrete CMS Security team CVSS scoring: 7.1 AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:HCredit for discovery: "Adrian Tiron from FORTBRIDGE (https://www.fortbridge.co.uk/)"This fix is also in Concrete version 9.0.0 **CVE ID : CVE-2021-22966**	g/developers/introduction/version-history/857-release-notes	
Authorization Bypass Through User-Controlled Key	19-Nov-21	5	In Concrete CMS (formerly concrete 5) below 8.5.7, IDOR Allows Unauthenticated User to Access Restricted Files If Allowed to Add Message to a Conversation.To remediate this, a check was added to verify a user has permissions to view files before attaching the files to a message in "add / edit message".Concrete CMS security team gave this a CVSS v3.1 score of 4.3 AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:NCredit for discovery Adrian H **CVE ID : CVE-2021-22967**	https://documentation.concretecms.org/developers/introduction/version-history/857-release-notes	A-CON-CONC-061221/114
N/A	19-Nov-21	6.5	A bypass of adding remote files in Concrete CMS (previously concrete5) File	https://documentation.concretecms.or	A-CON-CONC-061221/115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Manager leads to remote code execution in Concrete CMS (concrete5) versions 8.5.6 and below.The external file upload feature stages files in the public directory even if they have disallowed file extensions. They are stored in a directory with a random name, but it's possible to stall the uploads and brute force the directory name. You have to be an admin with the ability to upload files, but this bug gives you the ability to upload restricted file types and execute them depending on server configuration.To fix this, a check for allowed file extensions was added before downloading files to a tmp directory.Concrete CMS Security Team gave this a CVSS v3.1 score of 5.4 AV:N/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:NThis fix is also in Concrete version 9.0.0 **CVE ID : CVE-2021-22968**	g/developers/introduction/version-history/857-release-notes	
Server-Side Request Forgery (SSRF)	19-Nov-21	5	Concrete CMS (formerly concrete5) versions below 8.5.7 has a SSRF mitigation bypass using DNS Rebind attack giving an attacker the ability to fetch cloud IAAS (ex AWS) IAM keys.To fix this Concrete CMS no longer allows downloads from the local network and specifies the validated IP when downloading rather than	https://documentation.concretecms.org/developers/introduction/version-history/857-release-notes	A-CON-CONC-061221/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			relying on DNS.Discoverer: Adrian Tiron from FORTBRIDGE (https://www.fortbridge.co.uk/)The Concrete CMS team gave this a CVSS 3.1 score of 3.5 AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:N . Please note that Cloud IAAS provider mis-configurations are not Concrete CMS vulnerabilities. A mitigation for this vulnerability is to make sure that the IMDS configurations are according to a cloud provider's best practices.This fix is also in Concrete version 9.0.0 **CVE ID : CVE-2021-22969**		
Server-Side Request Forgery (SSRF)	19-Nov-21	5	Concrete CMS (formerly concrete5) versions 8.5.6 and below and version 9.0.0 allow local IP importing causing the system to be vulnerable toa. SSRF attacks on the private LAN servers by reading files from the local LAN. An attacker can pivot in the private LAN and exploit local network appsandb. SSRF Mitigation Bypass through DNS RebindingConcrete CMS security team gave this a CVSS score of 3.5 AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:NConcrete CMS is maintaining Concrete version 8.5.x until 1 May 2022 for security fixes.This CVE is	https://documentation.concretecms.org/developers/introduction/version-history/901-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/857-release-notes	A-CON-CONC-061221/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			shared with HackerOne Reports https://hackerone.com/reports/1364797 and https://hackerone.com/reports/1360016Reporters: Adrian Tiron from FORTBRIDGE (https://www.fortbridge.co.uk/) and Bipul Jaiswal **CVE ID : CVE-2021-22970**		
contest_gallery					
contest_gallery					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Nov-21	7.5	The Contest Gallery WordPress plugin before 13.1.0.6 does not have capability checks and does not sanitise or escape the cg-search-user-name-original parameter before using it in a SQL statement when exporting users from a gallery, which could allow unauthenticated to perform SQL injections attacks, as well as get the list of all users registered on the blog, including their username and email address **CVE ID : CVE-2021-24915**	N/A	A-CON-CONT-061221/118
creativemindssolutions					
video_lessons_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site	23-Nov-21	3.5	The Video Lessons Manager WordPress plugin before 1.7.2 and Video Lessons Manager Pro WordPress plugin before 3.5.9 do not properly sanitize and escape values when updating their settings, which	N/A	A-CRE-VIDE-061221/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			could allow high privilege users to perform Cross-Site Scripting attacks **CVE ID : CVE-2021-24713**		
video_lessons_manager_pro					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	3.5	The Video Lessons Manager WordPress plugin before 1.7.2 and Video Lessons Manager Pro WordPress plugin before 3.5.9 do not properly sanitize and escape values when updating their settings, which could allow high privilege users to perform Cross-Site Scripting attacks **CVE ID : CVE-2021-24713**	N/A	A-CRE-VIDE-061221/120
crocontrol					
asterix					
Out-of-bounds Read	22-Nov-21	6.4	Croatia Control Asterix 2.8.1 has a heap-based buffer over-read, with additional details to be disclosed at a later date. **CVE ID : CVE-2021-44144**	https://github.com/CroatiaControlLtd/asterix/issues/183	A-CRO-ASTE-061221/121
Darwin					
factor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-21	4.3	In Factor (App Framework & Headless CMS) forum plugin, versions 1.3.5 to 1.8.30, are vulnerable to reflected Cross-Site Scripting (XSS) at the "search" parameter in the URL. An unauthenticated attacker can execute malicious JavaScript code and steal the session cookies. **CVE ID : CVE-2021-25982**	https://github.com/FactorJS/factor/blob/v1.8.30/@plugins/plugin-forum/topic-list.vue#L139	A-DAR-FACT-061221/122
Improper	16-Nov-21	4.3	In Factor (App Framework &	https://gith	A-DAR-FACT-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			Headless CMS) forum plugin, versions v1.3.8 to v1.8.30, are vulnerable to reflected Cross-Site Scripting (XSS) at the "tags" and "category" parameters in the URL. An unauthenticated attacker can execute malicious JavaScript code and steal the session cookies. **CVE ID : CVE-2021-25983**	ub.com/FactorJS/factor/blob/v1.8.30/@plugins/plugin-forum/topic-list.vue#L141-L143	061221/123
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-21	4.3	In Factor (App Framework & Headless CMS) forum plugin, versions v1.3.3 to v1.8.30, are vulnerable to stored Cross-Site Scripting (XSS) at the "post reply" section. An unauthenticated attacker can execute malicious JavaScript code and steal the session cookies. **CVE ID : CVE-2021-25984**	https://github.com/FactorJS/factor/blob/v1.8.30/@plugins/plugin-forum/topic-reply.vue#L119	A-DAR-FACT-061221/124
Insufficient Session Expiration	16-Nov-21	7.5	In Factor (App Framework & Headless CMS) v1.0.4 to v1.8.30, improperly invalidate a user's session even after the user logs out of the application. In addition, user sessions are stored in the browser's local storage, which by default does not have an expiration time. This makes it possible for an attacker to steal and reuse the cookies using techniques such as XSS attacks, followed by a local account takeover. **CVE ID : CVE-2021-25985**	https://github.com/FactorJS/factor/blob/v1.8.30/@factor/user/util.ts#L65	A-DAR-FACT-061221/125
delitestudio					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
push_notifications_for_wordpress					
Cross-Site Request Forgery (CSRF)	24-Nov-21	6.8	Cross-site request forgery (CSRF) vulnerability in Push Notifications for WordPress (Lite) versions prior to 6.0.1 allows a remote attacker to hijack the authentication of an administrator and conduct an arbitrary operation via a specially crafted web page. **CVE ID : CVE-2021-20846**	https://delitestudio.com/en/	A-DEL-PUSH-061221/126
Dell					
cloudlink					
Use of Hard-coded Password	23-Nov-21	8.5	Dell EMC CloudLink 7.1 and all prior versions contain a Hard-coded Password Vulnerability. A remote high privileged attacker, with the knowledge of the hard-coded credentials, may potentially exploit this vulnerability to gain unauthorized access to the system. **CVE ID : CVE-2021-36312**	https://www.dell.com/support/kbdoc/en-us/000193031/https-dellservices-lightning-force-com-one-one-app	A-DEL-CLOU-061221/127
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Nov-21	9	Dell EMC CloudLink 7.1 and all prior versions contain an OS command injection Vulnerability. A remote high privileged attacker, may potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker. This vulnerability is	https://www.dell.com/support/kbdoc/en-us/000193031/https-dellservices-lightning-force-com-one-one-app	A-DEL-CLOU-061221/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			considered critical as it may be leveraged to completely compromise the vulnerable application as well as the underlying operating system. Dell recommends customers to upgrade at the earliest opportunity. **CVE ID : CVE-2021-36313**		
emc_cloud_link					
N/A	23-Nov-21	7.5	Dell EMC CloudLink 7.1 and all prior versions contain an Arbitrary File Creation Vulnerability. A remote unauthenticated attacker, may potentially exploit this vulnerability, leading to the execution of arbitrary files on the end user system. **CVE ID : CVE-2021-36314**	https://www.dell.com/support/kbdoc/en-us/000193031/https-dellservices-lightning-force-com-one-one-app	A-DEL-EMC_-061221/129
URL Redirection to Untrusted Site ('Open Redirect')	23-Nov-21	4.9	Dell EMC CloudLink 7.1 and all prior versions contain a HTML and Javascript Injection Vulnerability. A remote low privileged attacker, may potentially exploit this vulnerability, directing end user to arbitrary and potentially malicious websites. **CVE ID : CVE-2021-36332**	https://www.dell.com/support/kbdoc/en-us/000193031/https-dellservices-lightning-force-com-one-one-app	A-DEL-EMC_-061221/130
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Nov-21	2.1	Dell EMC CloudLink 7.1 and all prior versions contain a Buffer Overflow Vulnerability. A local low privileged attacker, may potentially exploit this vulnerability, leading to an application crash.	https://www.dell.com/support/kbdoc/en-us/000193031/https-dellservices-lightning-	A-DEL-EMC_-061221/131

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36333	force-com-one-one-apphttps://www.dell.com/support/kbdoc/en-us/000193031/https-dellservices-lightning-force-com-one-one-app	
Improper Neutralization of Formula Elements in a CSV File	23-Nov-21	6	Dell EMC CloudLink 7.1 and all prior versions contain a CSV formula Injection Vulnerability. A remote high privileged attacker, may potentially exploit this vulnerability, leading to arbitrary code execution on end user machine **CVE ID : CVE-2021-36334**	https://www.dell.com/support/kbdoc/en-us/000193031/https-dellservices-lightning-force-com-one-one-app	A-DEL-EMC_-061221/132
Improper Input Validation	23-Nov-21	6.5	Dell EMC CloudLink 7.1 and all prior versions contain an Improper Input Validation Vulnerability. A remote low privileged attacker, may potentially exploit this vulnerability, leading to execution of arbitrary files on the server **CVE ID : CVE-2021-36335**	https://www.dell.com/support/kbdoc/en-us/000193031/https-dellservices-lightning-force-com-one-one-app	A-DEL-EMC_-061221/133
emc_networker					
Incorrect Authorization	23-Nov-21	4.6	Dell EMC Networker versions prior to 19.5 contain an Improper Authorization vulnerability. Any local malicious user with networker user privileges	https://www.dell.com/support/kbdoc/000192419	A-DEL-EMC_-061221/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may exploit this vulnerability to upload malicious file to unauthorized locations and execute it. **CVE ID : CVE-2021-36311**		
emc_secure_connect_gateway					
Insertion of Sensitive Information into Log File	20-Nov-21	2.1	Dell EMC SCG 5.00.00.10 and earlier, contain a sensitive information disclosure vulnerability. A local malicious user may exploit this vulnerability to read sensitive information and use it. **CVE ID : CVE-2021-36340**	https://www.dell.com/support/kbdoc/en-us/000193601/dsa-2021-245-dell-emc-secure-connect-gateway-security-update-for-multiple-vulnerabilities	A-DEL-EMC_-061221/135
django-helpdesk_project					
django-helpdesk					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Nov-21	3.5	django-helpdesk is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-3950**	https://github.com/django-helpdesk/django-helpdesk/commit/04483bdac3b5196737516398b5ce0383875a5c60, https://huntr.dev/bounties/4d7a5fdd-b2de-467a-	A-DJA-DJAN-061221/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ade0-3f2fb386638e	
django-wiki_project					
django-wiki					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	3.5	In Django-wiki, versions 0.0.20 to 0.7.8 are vulnerable to Stored Cross-Site Scripting (XSS) in Notifications Section. An attacker who has access to edit pages can inject JavaScript payload in the title field. When a victim gets a notification regarding the changes made in the application, the payload in the notification panel renders and loads external JavaScript. **CVE ID : CVE-2021-25986**	https://github.com/django-wiki/django-wiki/commit/9eaccc7519e4206a4d2f22640882f0737b2da9c5	A-DJA-DJAN-061221/137
dotnetfoundation					
piranha_cms					
Cross-Site Request Forgery (CSRF)	16-Nov-21	4	In PiranhaCMS, versions 4.0.0-alpha1 to 9.2.0 are vulnerable to cross-site request forgery (CSRF) when performing various actions supported by the management system, such as deleting a user, deleting a role, editing a post, deleting a media folder etc., when an ID is known. **CVE ID : CVE-2021-25976**	https://github.com/PiranhaCMS/piranha.core/commit/e42abacdd0dd880ce9cf6607efcc24646ac82eda	A-DOT-PIRA-061221/138
Drupal					
drupal					
Improper Neutralizatio	17-Nov-21	3.5	CKEditor4 is an open source WYSIWYG HTML editor. In	https://github.com/cke	A-DRU-DRUP-061221/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			affected versions a vulnerability has been discovered in the Advanced Content Filter (ACF) module and may affect all plugins used by CKEditor 4. The vulnerability allowed to inject malformed HTML bypassing content sanitization, which could result in executing JavaScript code. It affects all users using the CKEditor 4 at version < 4.17.0. The problem has been recognized and patched. The fix will be available in version 4.17.0. **CVE ID : CVE-2021-41164**	ditor/ckeditor4/security/advisories/GHSA-pvmx-g8h5-cprj, https://github.com/ckeditor/ckeditor4/blob/major/CHANGES.md#ckeditor-417, https://www.drupal.org/sa-core-2021-011	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	3.5	CKEditor4 is an open source WYSIWYG HTML editor. In affected version a vulnerability has been discovered in the core HTML processing module and may affect all plugins used by CKEditor 4. The vulnerability allowed to inject malformed comments HTML bypassing content sanitization, which could result in executing JavaScript code. It affects all users using the CKEditor 4 at version < 4.17.0. The problem has been recognized and patched. The fix will be available in version 4.17.0. **CVE ID : CVE-2021-41165**	https://github.com/ckeditor/ckeditor4/security/advisories/GHSA-7h26-63m7-qhf2, https://www.drupal.org/sa-core-2021-011	A-DRU-DRUP-061221/140
duplicate_post_project					
duplicate_post					
Improper	19-Nov-21	9	The "Duplicate Post"	N/A	A-DUP-DUPL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			WordPress plugin up to and including version 1.1.9 is vulnerable to SQL Injection. SQL injection vulnerabilities occur when client supplied data is included within an SQL Query insecurely. SQL Injection can typically be exploited to read, modify and delete SQL table data. In many cases it also possible to exploit features of SQL server to execute system commands and/or access the local file system. This particular vulnerability can be exploited by any authenticated user who has been granted access to use the Duplicate Post plugin. By default, this is limited to Administrators, however the plugin presents the option to permit access to the Editor, Author, Contributor and Subscriber roles. **CVE ID : CVE-2021-43408**		061221/141
easyregistrationforms					
easy_registration_forms					
Cross-Site Request Forgery (CSRF)	19-Nov-21	6.8	The Easy Registration Forms WordPress plugin is vulnerable to Cross-Site Request Forgery due to missing nonce validation via the ajax_add_form function found in the ~/includes/class-form.php file which made it possible for attackers to inject arbitrary web scripts in versions up to,	N/A	A-EAS-EASY-061221/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and including 2.1.1. **CVE ID : CVE-2021-39353**		
Ec-cube					
ec-cube					
Incorrect Authorization	24-Nov-21	4	Improper access control in Management screen of EC-CUBE 2 series 2.11.2 to 2.17.1 allows a remote authenticated attacker to bypass access restriction and to alter System settings via unspecified vectors. **CVE ID : CVE-2021-20841**	https://www.ec-cube.net/info/weakness/20211111/	A-EC--EC-C-061221/143
Cross-Site Request Forgery (CSRF)	24-Nov-21	4.3	Cross-site request forgery (CSRF) vulnerability in EC-CUBE 2 series 2.11.0 to 2.17.1 allows a remote attacker to hijack the authentication of Administrator and delete Administrator via a specially crafted web page. **CVE ID : CVE-2021-20842**	https://www.ec-cube.net/info/weakness/20211111/	A-EC--EC-C-061221/144
edgexfoundry					
application_functions_software_development_kit					
Use of a Broken or Risky Cryptographic Algorithm	19-Nov-21	2.6	Functions SDK for EdgeX is meant to provide all the plumbing necessary for developers to get started in processing/transforming/exporting data out of the EdgeX IoT platform. In affected versions broken encryption in app-functions-sdk "AES" transform in EdgeX Foundry releases prior to Jakarta allows attackers to decrypt messages via unspecified vectors. The app-functions-	https://github.com/edgexfoundry/app-functions-sdk-go/commit/8fa13c6388ce76a6b878b54490eac61aa7d81165, https://github.com/edgexfoundry/a	A-EDG-APPL-061221/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sdk exports an “aes” transform that user scripts can optionally call to encrypt data in the processing pipeline. No decrypt function is provided. Encryption is not enabled by default, but if used, the level of protection may be less than the user may expects due to a broken implementation. Version v2.1.0 (EdgeX Foundry Jakarta release and later) of app-functions-sdk-go/v2 deprecates the “aes” transform and provides an improved “aes256” transform in its place. The broken implementation will remain in a deprecated state until it is removed in the next EdgeX major release to avoid breakage of existing software that depends on the broken implementation. As the broken transform is a library function that is not invoked by default, users who do not use the AES transform in their processing pipelines are unaffected. Those that are affected are urged to upgrade to the Jakarta EdgeX release and modify processing pipelines to use the new "aes256" transform. **CVE ID : CVE-2021-41278**	pp-functions-sdk-go/security/advisories/GHSA-6c7m-qwxj-mvhp	
app_service_configurable					
Use of a Broken or	19-Nov-21	2.6	Functions SDK for EdgeX is meant to provide all the	https://github.com/edg	A-EDG-APP_-061221/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Risky Cryptographic Algorithm			plumbing necessary for developers to get started in processing/transforming/exporting data out of the EdgeX IoT platform. In affected versions broken encryption in app-functions-sdk "AES" transform in EdgeX Foundry releases prior to Jakarta allows attackers to decrypt messages via unspecified vectors. The app-functions-sdk exports an "aes" transform that user scripts can optionally call to encrypt data in the processing pipeline. No decrypt function is provided. Encryption is not enabled by default, but if used, the level of protection may be less than the user may expects due to a broken implementation. Version v2.1.0 (EdgeX Foundry Jakarta release and later) of app-functions-sdk-go/v2 deprecates the "aes" transform and provides an improved "aes256" transform in its place. The broken implementation will remain in a deprecated state until it is removed in the next EdgeX major release to avoid breakage of existing software that depends on the broken implementation. As the broken transform is a library function that is not invoked by default, users who do not use the AES transform in their	exfoundry/app-functions-sdk-go/commit/8fa13c6388ce76a6b878b54490eac61aa7d81165, https://github.com/edgexfoundry/app-functions-sdk-go/security/advisories/GHSA-6c7m-qwxj-mvhp	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing pipelines are unaffected. Those that are affected are urged to upgrade to the Jakarta EdgeX release and modify processing pipelines to use the new "aes256" transform. **CVE ID : CVE-2021-41278**		
edgex_foundry					
Use of a Broken or Risky Cryptographic Algorithm	19-Nov-21	2.6	Functions SDK for EdgeX is meant to provide all the plumbing necessary for developers to get started in processing/transforming/exporting data out of the EdgeX IoT platform. In affected versions broken encryption in app-functions-sdk "AES" transform in EdgeX Foundry releases prior to Jakarta allows attackers to decrypt messages via unspecified vectors. The app-functions-sdk exports an "aes" transform that user scripts can optionally call to encrypt data in the processing pipeline. No decrypt function is provided. Encryption is not enabled by default, but if used, the level of protection may be less than the user may expects due to a broken implementation. Version v2.1.0 (EdgeX Foundry Jakarta release and later) of app-functions-sdk-go/v2 deprecates the "aes" transform and provides an improved "aes256" transform	https://github.com/edgexfoundry/app-functions-sdk-go/commit/8fa13c6388ce76a6b878b54490eac61aa7d81165, https://github.com/edgexfoundry/app-functions-sdk-go/security/advisories/GHSA-6c7m-qwxj-mvhp	A-EDG-EDGE-061221/147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in its place. The broken implementation will remain in a deprecated state until it is removed in the next EdgeX major release to avoid breakage of existing software that depends on the broken implementation. As the broken transform is a library function that is not invoked by default, users who do not use the AES transform in their processing pipelines are unaffected. Those that are affected are urged to upgrade to the Jakarta EdgeX release and modify processing pipelines to use the new "aes256" transform. **CVE ID : CVE-2021-41278**		
Elastic					
kibana					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Nov-21	4	It was discovered that on Windows operating systems specifically, Kibana was not validating a user supplied path, which would load .pbf files. Because of this, a malicious user could arbitrarily traverse the Kibana host to load internal files ending in the .pbf extension. Thanks to Dominic Couture for finding this vulnerability. **CVE ID : CVE-2021-37938**	https://discuss.elastic.co/t/kibana-7-15-2-security-update/288923	A-ELA-KIBA-061221/148
Cleartext Transmission of Sensitive	18-Nov-21	4	It was discovered that Kibana's JIRA connector & IBM Resilient connector could	https://discuss.elastic.co/t/kibana-7-	A-ELA-KIBA-061221/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			be used to return HTTP response data on internal hosts, which may be intentionally hidden from public view. Using this vulnerability, a malicious user with the ability to create connectors, could utilize these connectors to view limited HTTP response data on hosts accessible to the cluster. **CVE ID : CVE-2021-37939**	15-2-security-update/288923	
elementor					
website_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	4.3	The Elementor Website Builder WordPress plugin before 3.1.4 does not sanitise or escape user input appended to the DOM via a malicious hash, resulting in a DOM Cross-Site Scripting issue **CVE ID : CVE-2021-24891**	N/A	A-ELE-WEBS-061221/150
email_log_project					
email_log					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Nov-21	6.5	The Email Log WordPress plugin before 2.4.7 does not properly validate, sanitise and escape the "orderby" and "order" GET parameters before using them in SQL statement in the admin dashboard, leading to SQL injections **CVE ID : CVE-2021-24758**	N/A	A-EMA-EMAI-061221/151
emoji_button_project					
emoji_button					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Nov-21	4.3	@joeattardi/emoji-button is a Vanilla JavaScript emoji picker component. In affected versions there are two vectors for XSS attacks: a URL for a custom emoji, and an i18n string. In both of these cases, a value can be crafted such that it can insert a `script` tag into the page and execute malicious code. **CVE ID : CVE-2021-43785**	https://github.com/joeattardi/emoji-button/security/advisories/GHSA-f34m-x9pj-62vq, https://github.com/joeattardi/emoji-button/commit/05970c09180cd27fff493e998ac5bf0468b1bb16	A-EMO-EMOJ-061221/152
essentialplugin					
popup_anything					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	The Popup Anything WordPress plugin before 2.0.4 does not escape the Link Text and Button Text fields of Popup, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks **CVE ID : CVE-2021-24883**	https://plugins.trac.wordpress.org/changeset/2610975	A-ESS-POPU-061221/153
ethereum					
go_ethereum					
NULL Pointer Dereference	18-Nov-21	2.1	Go-Ethereum 1.10.9 nodes crash (denial of service) after receiving a serial of messages and cannot be recovered. They will crash with "runtime error: invalid memory address or nil pointer	N/A	A-ETH-GO_E-061221/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			dereference" and arise a SEGV signal. **CVE ID : CVE-2021-43668**		
F-secure					
atlant					
Improper Resource Shutdown or Release	26-Nov-21	4.3	A vulnerability affecting F-Secure antivirus engine was discovered whereby unpacking UPX file can lead to denial-of-service. The vulnerability can be exploited remotely by an attacker. A successful attack will result in denial-of-service of the antivirus engine. **CVE ID : CVE-2021-40833**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40833	A-F-S-ATLA-061221/155
elements_endpoint_protection					
Improper Resource Shutdown or Release	26-Nov-21	4.3	A vulnerability affecting F-Secure antivirus engine was discovered whereby unpacking UPX file can lead to denial-of-service. The vulnerability can be exploited remotely by an attacker. A successful attack will result in denial-of-service of the antivirus engine. **CVE ID : CVE-2021-40833**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business	A-F-S-ELEM-061221/156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/support-and-downloads/security-advisories/cve-2021-40833	
internet_gatekeeper					
Improper Resource Shutdown or Release	26-Nov-21	4.3	A vulnerability affecting F-Secure antivirus engine was discovered whereby unpacking UPX file can lead to denial-of-service. The vulnerability can be exploited remotely by an attacker. A successful attack will result in denial-of-service of the antivirus engine. **CVE ID : CVE-2021-40833**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40833	A-F-S-INTE-061221/157
linux_security					
Improper Resource Shutdown or Release	26-Nov-21	4.3	A vulnerability affecting F-Secure antivirus engine was discovered whereby unpacking UPX file can lead to denial-of-service. The vulnerability can be exploited remotely by an attacker. A successful attack will result in denial-of-service of the antivirus engine.	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-	A-F-S-LINU-061221/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40833	secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40833	
linux_security_64					
Improper Resource Shutdown or Release	26-Nov-21	4.3	A vulnerability affecting F-Secure antivirus engine was discovered whereby unpacking UPX file can lead to denial-of-service. The vulnerability can be exploited remotely by an attacker. A successful attack will result in denial-of-service of the antivirus engine. **CVE ID : CVE-2021-40833**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40833	A-F-S-LINU-061221/159
facade					
ignition					
N/A	17-Nov-21	7.5	The Ignition component before 1.16.15, and 2.0.x before 2.0.6, for Laravel has a "fix variable names" feature that can lead to incorrect access control. **CVE ID : CVE-2021-43996**	https://github.com/facade/ignition/compare/1.16.14...1.16.15, https://gith	A-FAC-IGNI-061221/160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ub.com/facade/ignition/pull/285, https://github.com/facade/ignition/compare/2.0.5...2.0.6	
feataholic					
maz_loader					
Cross-Site Request Forgery (CSRF)	23-Nov-21	4.3	The MAZ Loader WordPress plugin through 1.3.4 does not enforce nonce checks, which allows attackers to make administrators delete arbitrary loaders via a CSRF attack **CVE ID : CVE-2021-24668**	N/A	A-FEA-MAZ_-061221/161
Fedoraproject					
fedora_extra_packages_for_enterprise_linux					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-21	4.3	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. A URL parameter in the filetype site administrator tool required extra sanitizing to prevent a reflected XSS risk. **CVE ID : CVE-2021-43558**	https://moodle.org/mod/forum/discuss.php?d=429097	A-FED-FEDO-061221/162
Cross-Site Request Forgery (CSRF)	22-Nov-21	6.8	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. The "delete related badge" functionality did not include the necessary token check to prevent a CSRF risk.	https://moodle.org/mod/forum/discuss.php?d=429099	A-FED-FEDO-061221/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-43559		
Exposure of Resource to Wrong Sphere	22-Nov-21	5	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. Insufficient capability checks made it possible to fetch other users' calendar action events. **CVE ID : CVE-2021-43560**	https://moodle.org/mod/forum/discuss.php?d=429100	A-FED-FEDO-061221/164
gallagher					
command_centre					
Incorrect Comparison	18-Nov-21	5	An Incomplete Comparison with Missing Factors vulnerability in the Gallagher Controller allows an attacker to bypass PIV verification. This issue affects: Gallagher Command Centre 8.40 versions prior to 8.40.1888 (MR3); 8.30 versions prior to 8.30.1454 (MR3); 8.20 versions prior to 8.20.1291 (MR5); 8.10 versions prior to 8.10.1284 (MR7); version 8.00 and prior versions. **CVE ID : CVE-2021-23146**	https://security.gallagher.com/Security-Advisories/CVE-2021-23146	A-GAL-COMM-061221/165
Improper Certificate Validation	18-Nov-21	4.3	Improper certificate validation vulnerability in SMTP Client allows man-in-the-middle attack to retrieve sensitive information from the Command Centre Server. This issue affects: Gallagher Command Centre 8.50 versions prior to 8.50.2048 (MR3); 8.40 versions prior to 8.40.2063 (MR4); 8.30 versions prior to 8.30.1454 (MR4) ; version 8.20 and	https://security.gallagher.com/Security-Advisories/CVE-2021-23167	A-GAL-COMM-061221/166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior versions. **CVE ID : CVE-2021-23167**		
Improper Privilege Management	18-Nov-21	4	Improper privilege validation vulnerability in COM Interface of Gallagher Command Centre Server allows authenticated unprivileged operators to retrieve sensitive information from the Command Centre Server. This issue affects: Gallagher Command Centre 8.50 versions prior to 8.50.2048 (MR3) ; 8.40 versions prior to 8.40.2063 (MR4); 8.30 versions prior to 8.30.1454 (MR4) ; 8.20 versions prior to 8.20.1291 (MR6); version 8.10 and prior versions. **CVE ID : CVE-2021-23193**	https://security.gallagher.com/Security-Advisories/CVE-2021-23193	A-GAL-COMM-061221/167
Unquoted Search Path or Element	18-Nov-21	4.6	Unquoted service path vulnerability in the Gallagher Controller Service allows an unprivileged user to execute arbitrary code as the account that runs the Controller Service. This issue affects: Gallagher Command Centre 8.50 versions prior to 8.50.2048 (MR3) ; **CVE ID : CVE-2021-23197**	https://security.gallagher.com/Security-Advisories/CVE-2021-23197	A-GAL-COMM-061221/168
command_centre_mobile_client					
Improper Certificate Validation	18-Nov-21	4.3	Improper validation of the cloud certificate chain in Mobile Client allows man-in-the-middle attack to impersonate the legitimate Command Centre Server. This issue affects: Gallagher	https://security.gallagher.com/Security-Advisories/CVE-2021-23155	A-GAL-COMM-061221/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Command Centre Mobile Client for Android 8.60 versions prior to 8.60.065; version 8.50 and prior versions. **CVE ID : CVE-2021-23155**		
command_centre_mobile_connect					
Improper Certificate Validation	18-Nov-21	6.8	Improper validation of the cloud certificate chain in Mobile Connect allows man-in-the-middle attack to impersonate the legitimate Command Centre Server. This issue affects: Gallagher Command Centre Mobile Connect for Android 15 versions prior to 15.04.040; version 14 and prior versions. **CVE ID : CVE-2021-23162**	https://security.gallagher.com/Security-Advisories/CVE-2021-23162	A-GAL-COMM-061221/170
generateblocks					
generateblocks					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	The GenerateBlocks WordPress plugin before 1.4.0 does not validate the generateblocks/container block's tagName attribute, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks. **CVE ID : CVE-2021-24751**	N/A	A-GEN-GENE-061221/171
gerbv_project					
gerbv					
Out-of-bounds Write	19-Nov-21	7.5	An out-of-bounds write vulnerability exists in the drill format T-code tool number functionality of Gerbv 2.7.0,	N/A	A-GER-GERB-061221/172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			dev (commit b5f1eacd), and the forked version of Gerbv (commit 71493260). A specially-crafted drill file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-40391**		
gesundheit-bewegt					
colorful_categories					
Cross-Site Request Forgery (CSRF)	17-Nov-21	4.3	The Colorful Categories WordPress plugin before 2.0.15 does not enforce nonce checks which could allow attackers to make a logged in admin or editor change taxonomy colors via a CSRF attack **CVE ID : CVE-2021-24802**	N/A	A-GES-COLO-061221/173
getgrav					
grav-plugin-admin					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Nov-21	3.5	grav-plugin-admin is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-3920**	https://github.com/getgrav/grav-plugin-admin/commit/6463135bf046d8131189c163158cd5db8f7a9675, https://hunt r.dev/bounties/ab564760-90c6-4e1d-80c2-852f45034c	A-GET-GRAV-061221/174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				d1	
Getkirby					
Kirby					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-21	2.1	Kirby is an open source file structured CMS ### Impact Kirby's writer field stores its formatted content as HTML code. Unlike with other field types, it is not possible to escape HTML special characters against cross-site scripting (XSS) attacks, otherwise the formatting would be lost. If the user is logged in to the Panel, a harmful script can for example trigger requests to Kirby's API with the permissions of the victim. Because the writer field did not securely sanitize its contents on save, it was possible to inject malicious HTML code into the content file by sending it to Kirby's API directly without using the Panel. This malicious HTML code would then be displayed on the site frontend and executed in the browsers of site visitors and logged in users who are browsing the site. Attackers must be in your group of authenticated Panel users in order to exploit this weakness. Users who do not make use of the writer field are not affected. This issue has been patched in Kirby 3.5.8 by sanitizing all writer	https://github.com/getkirby/kirby/security/advisories/GHSA-x7j7-qp7j-hw3q, https://github.com/getkirby/kirby/commit/25fc5c6b330442e6433c99befc688f3698c5d1fc	A-GET-KIRB-061221/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			field contents on the backend whenever the content is modified via Kirby's API. Please update to this or a later version to fix the vulnerability. **CVE ID : CVE-2021-41252**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-21	2.1	Kirby is an open source file structured CMS. In affected versions Kirby's blocks field stores structured data for each block. This data is then used in block snippets to convert the blocks to HTML for use in your templates. We recommend to escape HTML special characters to protect against cross-site scripting (XSS) attacks. The default snippet for the image block unfortunately did not use our escaping helper. This made it possible to include malicious HTML code in the source, alt and link fields of the image block, which would then be displayed on the site frontend and executed in the browsers of site visitors and logged in users who are browsing the site. Attackers must be in your group of authenticated Panel users in order to exploit this weakness. Users who do not make use of the blocks field are not affected. This issue has been patched in Kirby version 3.5.8 by escaping special HTML characters in the output from the default	https://github.com/getkirby/kirby/pull/3510, https://github.com/getkirby/kirby/security/advisories/GHSA-cq58-r77c-5jjw	A-GET-KIRB-061221/176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			image block snippet. Please update to this or a later version to fix the vulnerability. **CVE ID : CVE-2021-41258**		
gin-vue-admin_project					
gin-vue-admin					
N/A	24-Nov-21	7.5	Gin-Vue-Admin before 2.4.6 mishandles a SQL database. **CVE ID : CVE-2021-44219**	https://github.com/flipped-aurora/gin-vue-admin/issues/813, https://github.com/flipped-aurora/gin-vue-admin/pull/811	A-GIN-GIN--061221/177
GNU					
binutils					
Use After Free	18-Nov-21	7.5	GCC c++filt v2.26 was discovered to contain a use-after-free vulnerability via the component cplus-dem.c. **CVE ID : CVE-2021-37322**	https://gcc.gnu.org/bugzilla/show_bug.cgi?id=99188	A-GNU-BINU-061221/178
gcc					
Use After Free	18-Nov-21	7.5	GCC c++filt v2.26 was discovered to contain a use-after-free vulnerability via the component cplus-dem.c. **CVE ID : CVE-2021-37322**	https://gcc.gnu.org/bugzilla/show_bug.cgi?id=99188	A-GNU-GCC-061221/179
Google					
chrome					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	23-Nov-21	6.8	Use after free in Sign-In in Google Chrome prior to 95.0.4638.69 allowed a remote attacker who convinced a user to sign into Chrome to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37997**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html, https://crbug.com/1259864	A-GOO-CHRO-061221/180
Use After Free	23-Nov-21	6.8	Use after free in Garbage Collection in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37998**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html, https://crbug.com/1259587	A-GOO-CHRO-061221/181
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	4.3	Insufficient data validation in New Tab Page in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to inject arbitrary scripts or HTML in a new browser tab via a crafted HTML page. **CVE ID : CVE-2021-37999**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html, https://crbug.com/1251541	A-GOO-CHRO-061221/182
Improper Input Validation	23-Nov-21	5.8	Insufficient validation of untrusted input in Intents in Google Chrome on Android prior to 95.0.4638.69 allowed	https://crbug.com/1249962, https://chro	A-GOO-CHRO-061221/183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a remote attacker to arbitrarily browser to a malicious URL via a crafted HTML page. **CVE ID : CVE-2021-38000**	mereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html	
Access of Resource Using Incompatible Type ('Type Confusion')	23-Nov-21	6.8	Type confusion in V8 in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-38001**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html, https://crbug.com/1260577	A-GOO-CHRO-061221/184
Use After Free	23-Nov-21	6.8	Use after free in Web Transport in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2021-38002**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html, https://crbug.com/1260940	A-GOO-CHRO-061221/185
Out-of-bounds Write	23-Nov-21	6.8	Inappropriate implementation in V8 in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.	A-GOO-CHRO-061221/186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-38003	html, https://crbug.com/1263462	
Exposure of Resource to Wrong Sphere	23-Nov-21	4.3	Insufficient policy enforcement in Autofill in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-38004**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html, https://crbug.com/1227170	A-GOO-CHRO-061221/187
greenplum					
greenplum					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Nov-21	6.4	In versions of Greenplum database prior to 5.28.6 and 6.14.0, greenplum database contains a file path traversal vulnerability leading to information disclosure from the file system. A malicious user can read/write information from the file system using this vulnerability. **CVE ID : CVE-2021-22028**	https://github.com/greenplum-db/gpdb/security/advisories/GHSA-hqh5-m87w-57w2	A-GRE-GREE-061221/188
Insertion of Sensitive Information into Log File	19-Nov-21	4	In versions of Greenplum database prior to 5.28.14 and 6.17.0, certain statements execution led to the storage of sensitive(credential) information in the logs of the database. A malicious user with access to logs can read sensitive(credentials)	https://github.com/greenplum-db/gpdb/security/advisories/GHSA-c7w8-gx27-h4mr	A-GRE-GREE-061221/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about users **CVE ID : CVE-2021-22030**		
hashicorp					
vault					
Incorrect Permission Assignment for Critical Resource	30-Nov-21	6.4	HashiCorp Vault and Vault Enterprise 0.11.0 up to 1.7.5 and 1.8.4 templated ACL policies would always match the first-created entity alias if multiple entity aliases exist for a specified entity and mount combination, potentially resulting in incorrect policy enforcement. Fixed in Vault and Vault Enterprise 1.7.6, 1.8.5, and 1.9.0. **CVE ID : CVE-2021-43998**	https://discuss.hashicorp.com/t/hcsec-2021-30-vaults-templated-acl-policies-matched-first-created-alias-per-entity-and-auth-backend/32132	A-HAS-VAUL-061221/190
helpful_project					
helpful					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	3.5	The Helpful WordPress plugin before 4.4.59 does not sanitise and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24841**	N/A	A-HEL-HELP-061221/191
hexo					
hexo					
Improper Neutralization of Input During Web	30-Nov-21	1.9	Hexo versions 0.0.1 to 5.4.0 are vulnerable against stored XSS. The post “body” and “tags” don’t sanitize malicious	https://github.com/hexojs/hexo/commit/5170d	A-HEX-HEXO-061221/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			javascript during web page generation. Local unprivileged attacker can inject arbitrary code. **CVE ID : CVE-2021-25987**	f2d3fa9c69e855c4b7c2b084ebfd92d5200	
hitachienergy					
counterparty_settlements_and_billing					
Improper Authentication	17-Nov-21	3.6	Improper Access Control vulnerability in the application authentication and authorization of Hitachi Energy Retail Operations, Counterparty Settlement and Billing (CSB) allows an attacker to execute a modified signed Java Applet JAR file. A successful exploitation may lead to data extraction or modification of data inside the application. This issue affects: Hitachi Energy Retail Operations 5.7.3 and prior versions. Hitachi Energy Counterparty Settlement and Billing (CSB) 5.7.3 prior versions. **CVE ID : CVE-2021-35528**	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000068&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000067&LanguageCode=en&DocumentPartId=&Action=Launch	A-HIT-COUN-061221/193
retail_operations					
Improper Authentication	17-Nov-21	3.6	Improper Access Control vulnerability in the application authentication and authorization of Hitachi Energy Retail Operations, Counterparty Settlement and Billing (CSB) allows an attacker to execute a modified signed Java Applet JAR file. A	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000068&LanguageCode=en&DocumentPart	A-HIT-RETA-061221/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploitation may lead to data extraction or modification of data inside the application. This issue affects: Hitachi Energy Retail Operations 5.7.3 and prior versions. Hitachi Energy Counterparty Settlement and Billing (CSB) 5.7.3 prior versions. **CVE ID : CVE-2021-35528**	Id=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000067&LanguageCode=en&DocumentPartId=&Action=Launch	
html2csv_project					
html2csv					
Improper Neutralization of Formula Elements in a CSV File	26-Nov-21	7.5	This affects all versions of package html-to-csv. When there is a formula embedded in a HTML page, it gets accepted without any validation and the same would be pushed while converting it into a CSV file. Through this a malicious actor can embed or generate a malicious link or execute commands via CSV files. **CVE ID : CVE-2021-23654**	https://snyk.io/vuln/SNYK-PYTHON-HTMLTOCSV-1582784, https://github.com/hanwentao/html2csv/blob/master/html2csv/converter.py	A-HTM-HTML-061221/195
Huawei					
emui					
N/A	23-Nov-21	5	There is an Identity verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability. **CVE ID : CVE-2021-37029**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-EMUI-061221/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	23-Nov-21	5	There is an Improper permission vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability. **CVE ID : CVE-2021-37030**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-EMUI-061221/197
N/A	23-Nov-21	5	There is a Remote DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the app to exit unexpectedly. **CVE ID : CVE-2021-37031**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-EMUI-061221/198
N/A	23-Nov-21	5	There is a Bypass vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause Digital Balance to fail to work. **CVE ID : CVE-2021-37032**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-EMUI-061221/199
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Nov-21	5	There is an Injection attack vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability. **CVE ID : CVE-2021-37033**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-EMUI-061221/200
N/A	23-Nov-21	5	There is an Unstandardized field names in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2021-37034**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-EMUI-061221/201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Nov-21	5	There is a Remote DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the app to exit unexpectedly. **CVE ID : CVE-2021-37035**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-EMUI-061221/202
fusioncompute					
Exposure of Sensitive Information to an Unauthorized Actor	23-Nov-21	2.1	There is an information leakage vulnerability in FusionCompute 6.5.1, eCNS280_TD V100R005C00 and V100R005C10. Due to the improperly storage of specific information in the log file, the attacker can obtain the information when a user logs in to the device. Successful exploit may cause the information leak. **CVE ID : CVE-2021-37036**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210818-01-informationleak-en	A-HUA-FUSI-061221/203
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Nov-21	9	There is a command injection vulnerability in CMA service module of FusionCompute product when processing the default certificate file. The software constructs part of a command using external special input from users, but the software does not sufficiently validate the user input. Successful exploit could allow the attacker to inject certain commands to the system. Affected product versions include: FusionCompute 6.0.0, 6.3.0, 6.3.1, 6.5.0, 6.5.1, 8.0.0. **CVE ID : CVE-2021-37102**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210922-01-cmd-en	A-HUA-FUSI-061221/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
magic_ui					
N/A	23-Nov-21	5	There is an Identity verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability. **CVE ID : CVE-2021-37029**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-MAGI-061221/205
Incorrect Default Permissions	23-Nov-21	5	There is an Improper permission vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability. **CVE ID : CVE-2021-37030**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-MAGI-061221/206
N/A	23-Nov-21	5	There is a Remote DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the app to exit unexpectedly. **CVE ID : CVE-2021-37031**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-MAGI-061221/207
N/A	23-Nov-21	5	There is a Bypass vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause Digital Balance to fail to work. **CVE ID : CVE-2021-37032**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-MAGI-061221/208
Improper Neutralization of Special Elements in Output Used by a Downstream	23-Nov-21	5	There is an Injection attack vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability. **CVE ID : CVE-2021-37033**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-MAGI-061221/209

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')					
N/A	23-Nov-21	5	There is an Unstandardized field names in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2021-37034**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-MAGI-061221/210
N/A	23-Nov-21	5	There is a Remote DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the app to exit unexpectedly. **CVE ID : CVE-2021-37035**	https://consumer.huawei.com/en/support/bulletin/2021/8/	A-HUA-MAGI-061221/211
IBM					
iris_xe_max_dedicated_graphics					
Improper Privilege Management	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Iris(R) Xe MAX Dedicated Graphics Drivers for Windows 10 before version 27.20.100.9466 may allow authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0121**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00566.html	A-IBM-IRIS-061221/212
mq					
N/A	23-Nov-21	4	IBM MQ 8.0, 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.1 CD, and 9.2 CD is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 208398. **CVE ID : CVE-2021-38875**	https://exchange.xforce.ibmcloud.com/vulnerabilities/208398, https://www.ibm.com/support/page	A-IBM-MQ-061221/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				s/node/6517672	
Cleartext Storage of Sensitive Information	16-Nov-21	2.1	IBM MQ 7.5, 8.0, 9.0 LTS, 9.1 CD, and 9.1 LTS stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 211403. **CVE ID : CVE-2021-38949**	https://www.ibm.com/support/pages/node/6516424	A-IBM-MQ-061221/214
mq_appliance					
N/A	30-Nov-21	2.1	IBM MQ Appliance 9.2 CD and 9.2 LTS is affected by a denial of service attack caused by a concurrency issue. IBM X-Force ID: 212042 **CVE ID : CVE-2021-38958**	https://www.ibm.com/support/pages/node/6519420, https://exchange.xforce.ibmcloud.com/vulnerabilities/212043	A-IBM-MQ_A-061221/215
Improper Control of Generation of Code ('Code Injection')	30-Nov-21	4.6	IBM MQ Appliance 9.2 CD and 9.2 LTS could allow a local privileged user to inject and execute malicious code. IBM X-Force ID: 212441. **CVE ID : CVE-2021-38967**	https://exchange.xforce.ibmcloud.com/vulnerabilities/212441, https://www.ibm.com/support/pages/node/6512826	A-IBM-MQ_A-061221/216
Exposure of Sensitive Information to an Unauthorized Actor	30-Nov-21	2.1	IBM MQ Appliance could allow a local attacker to obtain sensitive information by inclusion of sensitive data within trace. **CVE ID : CVE-2021-38999**	https://exchange.xforce.ibmcloud.com/vulnerabilities/213214, https://www.ibm.com/s	A-IBM-MQ_A-061221/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				upport/pages/node/6519418	
Exposure of Sensitive Information to an Unauthorized Actor	30-Nov-21	2.1	IBM MQ Appliance 9.2 CD and 9.2 LTS could allow a local attacker to obtain sensitive information by inclusion of sensitive data within diagnostics. IBM X-Force ID: 213215. **CVE ID : CVE-2021-39000**	https://www.ibm.com/support/pages/node/6519422, https://exchange.xforce.ibmcloud.com/vulnerabilities/213215	A-IBM-MQ_A-061221/218
planning_analytics					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-Nov-21	9.3	IBM Planning Analytics 2.0 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 208396. **CVE ID : CVE-2021-38873**	https://www.ibm.com/support/pages/node/6517470, https://exchange.xforce.ibmcloud.com/vulnerabilities/208396	A-IBM-PLAN-061221/219
security_guardium_key_lifecycle_manager					
Generation of Error Message Containing Sensitive Information	23-Nov-21	5	IBM Tivoli Key Lifecycle Manager (IBM Security Guardium Key Lifecycle Manager) 3.0, 3.0.1, 4.0, and 4.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID:	https://exchange.xforce.ibmcloud.com/vulnerabilities/212786, https://www.ibm.com/support/pages/node/6518326	A-IBM-SECU-061221/220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212786. **CVE ID : CVE-2021-38980**		
security_key_lifecycle_manager					
Generation of Error Message Containing Sensitive Information	23-Nov-21	5	IBM Tivoli Key Lifecycle Manager (IBM Security Guardium Key Lifecycle Manager) 3.0, 3.0.1, 4.0, and 4.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 212786. **CVE ID : CVE-2021-38980**	https://exchange.xforce.ibmcloud.com/vulnerabilities/212786, https://www.ibm.com/support/pages/node/6518326	A-IBM-SECU-061221/221
spectrum_scale					
N/A	16-Nov-21	2.1	IBM Spectrum Scale 5.1.0 through 5.1.1.1 could allow a privileged admin to destroy filesystem audit logging records before expiration time. IBM X-Force ID: 209164. **CVE ID : CVE-2021-38882**	https://www.ibm.com/support/pages/node/6516426	A-IBM-SPEC-061221/222
spss_statistics					
Out-of-bounds Write	17-Nov-21	2.1	IBM SPSS Statistics for Windows 24.0, 25.0, 26.0, 27.0, 27.0.1, and 28.0 could allow a local user to cause a denial of service by writing arbitrary files to admin protected directories on the system. IBM X-Force ID: 212046. **CVE ID : CVE-2021-38959**	https://exchange.xforce.ibmcloud.com/vulnerabilities/212046, https://www.ibm.com/support/pages/node/6516680	A-IBM-SPSS-061221/223
sterling_connect					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	23-Nov-21	5	IBM Sterling Connect:Direct Web Services 1.0 and 6.0 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 209507. **CVE ID : CVE-2021-38890**	https://www.ibm.com/support/pages/node/6518586, https://exchange.xforce.ibmcloud.com/vulnerabilities/209507	A-IBM-STER-061221/224
Inadequate Encryption Strength	23-Nov-21	5	IBM Sterling Connect:Direct Web Services 1.0 and 6.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 209508. **CVE ID : CVE-2021-38891**	https://www.ibm.com/support/pages/node/6518582, https://exchange.xforce.ibmcloud.com/vulnerabilities/209508	A-IBM-STER-061221/225
vios					
N/A	17-Nov-21	2.1	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the libc.a library to expose sensitive information. IBM X-Force ID: 206084. **CVE ID : CVE-2021-29860**	https://www.ibm.com/support/pages/node/6516774, https://exchange.xforce.ibmcloud.com/vulnerabilities/206084	A-IBM-VIOS-061221/226
N/A	17-Nov-21	2.1	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in EFS to expose sensitive information. IBM X-	https://exchange.xforce.ibmcloud.com/vulnerabilities/206085,	A-IBM-VIOS-061221/227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Force ID: 206085. **CVE ID : CVE-2021-29861**	https://www.ibm.com/support/pages/node/6516786	
websphere_mq					
Cleartext Storage of Sensitive Information	16-Nov-21	2.1	IBM MQ 7.5, 8.0, 9.0 LTS, 9.1 CD, and 9.1 LTS stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 211403. **CVE ID : CVE-2021-38949**	https://www.ibm.com/support/pages/node/6516424	A-IBM-WEBS-061221/228
imageboss					
imageboss					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	3.5	The ImageBoss WordPress plugin before 3.0.6 does not sanitise and escape its Source Name setting, which could allow high privilege users to perform Cross-Site Scripting attacks **CVE ID : CVE-2021-24888**	N/A	A-IMA-IMAG-061221/229
Imagemagick					
imagemagick					
Use After Free	19-Nov-21	6.8	A flaw was found in ImageMagick where it did not properly sanitize certain input before using it to invoke convert processes. This flaw allows an attacker to create a specially crafted image that leads to a use-after-free vulnerability when processed by ImageMagick. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	https://bugzilla.redhat.com/show_bug.cgi?id=2023196, https://github.com/ImageMagick/ImageMagick/commit/82775af03bbb10a0a1d0e15c0156c756	A-IMA-IMAG-061221/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-3962	73b4525e	
imagestowebp_project					
images_to_webp					
Cross-Site Request Forgery (CSRF)	23-Nov-21	5.8	The Images to WebP WordPress plugin before 1.9 does not have CSRF checks in place when performing some administrative actions, which could result in modification of plugin settings, Denial-of-Service, as well as arbitrary image conversion **CVE ID : CVE-2021-24641**	N/A	A-IMA-IMAG-061221/231
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-21	5	The Images to WebP WordPress plugin before 1.9 does not validate or sanitise the tab parameter before passing it to the include() function, which could lead to a Local File Inclusion issue **CVE ID : CVE-2021-24644**	N/A	A-IMA-IMAG-061221/232
implecode					
ecommerce_product_catalog					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	4.3	The eCommerce Product Catalog Plugin for WordPress plugin before 3.0.39 does not escape the ic-settings-search parameter before outputting it back in the page in an attribute, leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24875**	N/A	A-IMP-ECOM-061221/233
reviews_plus					
Uncontrolled Resource Consumption	23-Nov-21	4	The Reviews Plus WordPress plugin before 1.2.14 does not validate the submitted rating,	https://plugins.trac.wordpress.org/c	A-IMP-REVI-061221/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowing submission of long integer, causing a Denial of Service in the review section when an authenticated user submit such rating and the reviews are set to be displayed on the post/page **CVE ID : CVE-2021-24894**	hangeset/2618234	
incsub					
forminator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	3.5	The Forminator WordPress plugin before 1.15.4 does not sanitize and escape the email field label, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed **CVE ID : CVE-2021-24700**	N/A	A-INC-FORM-061221/235
infornweb					
logo_showcase_with_slick_slider					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	3.5	The Logo Showcase with Slick Slider WordPress plugin before 1.2.4 does not sanitise the Grid Settings, which could allow users with a role as low as Author to perform stored Cross-Site Scripting attacks via post metadata of Grid logo showcase. **CVE ID : CVE-2021-24729**	N/A	A-INF-LOGO-061221/236
insert_pages_project					
insert_pages					
Improper Neutralization of Input During Web	17-Nov-21	3.5	The Insert Pages WordPress plugin before 3.7.0 adds a shortcode that prints out other pages' content and	N/A	A-INS-INSE-061221/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			custom fields. It can be used by users with a role as low as Contributor to perform Cross-Site Scripting attacks by storing the payload/s in another post's custom fields. **CVE ID : CVE-2021-24850**		
Incorrect Authorization	17-Nov-21	4	The Insert Pages WordPress plugin before 3.7.0 allows users with a role as low as Contributor to access content and metadata from arbitrary posts/pages regardless of their author and status (ie private), using a shortcode. Password protected posts/pages are not affected by such issue. **CVE ID : CVE-2021-24851**	https://plugins.trac.wordpress.org/changeset/2614442/insert-pages	A-INS-INSE-061221/238
Intel					
administrative_tools_for_intel_network_adapters					
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer Intel(R)Administrative Tools for Intel(R) Network Adaptersfor Windowsbefore version 1.4.0.21 may allow an unauthenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33058**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00555.html	A-INT-ADMI-061221/239
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) Administrative Tools for Intel(R) Network Adapters driver for Windows before version 1.4.0.15, may allow a privileged user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	A-INT-ADMI-061221/240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2021-33059**	00555.html	
crypto_api_toolkit_for_intel_sgx					
Time-of-check Time-of-use (TOCTOU) Race Condition	17-Nov-21	6	Time-of-check time-of-use vulnerability in the Crypto API Toolkit for Intel(R) SGX may allow a privileged user to potentially enable escalation of privilege via network access. **CVE ID : CVE-2021-33097**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00565.html	A-INT-CRYP-061221/241
distribution_of_openvino_toolkit					
Uncontrolled Resource Consumption	17-Nov-21	2.1	Uncontrolled resource consumption in the Intel(R) Distribution of OpenVINOâ„¢ Toolkit before version 2021.4 may allow an unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33073**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00538.html	A-INT-DIST-061221/242
endpoint_management_assistant					
Improper Input Validation	17-Nov-21	5	Improper input validation for Intel(R) EMA before version 1.5.0 may allow an unauthenticated user to potentially enable denial of service via network access. **CVE ID : CVE-2021-0013**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00482.html	A-INT-ENDP-061221/243
ethernet_500_series_controllers_driver					
Improper Input Validation	17-Nov-21	4.9	Improper input validation in the Intel(R) Ethernet ixgbe driver for Linux before version 3.17.3 may allow an authenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advis	A-INT-ETHE-061221/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2021-33098**	ory/intel-sa-00555.html	
ethernet_diagnostic_driver					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) Ethernet Diagnostic Driver for Windows before version 1.4.0.10 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0135**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00524.html	A-INT-ETHE-061221/245
graphics_driver					
Improper Initialization	17-Nov-21	2.1	Improper initialization in the installer for some Intel(R) Graphics DCH Drivers for Windows 10 before version 27.20.100.9316 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0120**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00566.html	A-INT-GRAP-061221/246
hardware_accelerated_execution_manager					
Uncontrolled Resource Consumption	17-Nov-21	4.6	Uncontrolled resource consumption in the Intel(R) HAXM software before version 7.6.6 may allow an unauthenticated user to potentially enable privilege escalation via local access. **CVE ID : CVE-2021-0180**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00544.html	A-INT-HARD-061221/247
Uncontrolled Resource Consumption	17-Nov-21	2.1	Uncontrolled resource consumption in the Intel(R) HAXM software before version 7.6.6 may allow an unauthenticated user to potentially enable information disclosure via	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	A-INT-HARD-061221/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2021-0182**	00544.html	
nuc_hdmi_firmware_update_tool					
Improper Privilege Management	17-Nov-21	4.6	Improper access control in the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC8i3BE, NUC8i5BE, NUC8i7BE before version 1.78.4.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33089**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	A-INT-NUC_-061221/249
Incorrect Default Permissions	17-Nov-21	7.2	Incorrect default permissionsin the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC10i3FN, NUC10i5FN, NUC10i7FN before version 1.78.2.0.7 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33090**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	A-INT-NUC_-061221/250
oneapi_rendering_toolkit					
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the installer for the Intel(R) oneAPI Rendering Toolkit before version 2021.2 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00564.html	A-INT-ONEA-061221/251
realsense_d400_series_universal_windows_platform_driver					
Untrusted Search Path	17-Nov-21	4.4	Uncontrolled search path in the Intel(R) RealSense(TM) D400 Series UWP driver for Windows 10 before version	https://www.intel.com/content/www/us/en/se	A-INT-REAL-061221/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.1.160.22 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33063**	curity-center/advisory/intel-sa-00557.html	
safestring_library					
Integer Overflow or Wraparound	17-Nov-21	4.6	Integer overflow in the Safestring library maintained by Intel(R) may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33106**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00584.html	A-INT-SAFE-061221/253
serial_io_driver_for_intel_nuc_11_gen					
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the software installer for the Intel(R) Serial IO driver for Intel(R) NUC 11 Gen before version 30.100.2104.1 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33118**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00560.html	A-INT-SERI-061221/254
sgx_sdk					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	A-INT-SGX_-061221/255
thunderbolt_dch_driver					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows	https://www.intel.com/content/ww	A-INT-THUN-061221/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	w/us/en/security-center/advisory/intel-sa-00533.html	
vtune_profiler					
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the software installer for the Intel(R) VTune(TM) Profiler before version 2021.3.0 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33062**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00556.html	A-INT-VTUN-061221/257
ionic					
identity_vault					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	4.6	In Ionic Identity Vault before 5.0.5, the protection mechanism for invalid unlock attempts can be bypassed. **CVE ID : CVE-2021-44033**	https://ionic.io/docs/identity-vault/changelog	A-ION-IDEN-061221/258
ipack					
scada_automation					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Nov-21	7.5	Due to improper sanitization iPack SCADA Automation software suffers from a remote SQL injection vulnerability. An unauthenticated attacker with the web access is able to extract critical information from the system. **CVE ID : CVE-2021-3958**	N/A	A-IPA-SCAD-061221/259
ipuptime					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pinkie					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Nov-21	5	Pinkie 2.15 allows remote attackers to cause a denial of service (daemon crash) via a TFTP read (RRQ) request, aka opcode 1. **CVE ID : CVE-2021-44428**	N/A	A-IPU-PINK-061221/260
issabel					
pbx					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	4.3	An unspecified version of issabelPBX is affected by a Cross Site Scripting (XSS) vulnerability. In file page.backup_restore.php, the exit function will terminate the script and print the message to the user. The message will contain $_REQUEST without sanitization, then there is a XSS vulnerability. **CVE ID : CVE-2021-43695**	N/A	A-ISS-PBX-061221/261
isync_project					
isync					
Out-of-bounds Write	22-Nov-21	7.5	A flaw was found in mbsync in isync 1.4.0 through 1.4.3. Due to an unchecked condition, a malicious or compromised IMAP server could use a crafted mail message that lacks headers (i.e., one that starts with an empty line) to provoke a heap overflow, which could conceivably be exploited for remote code execution. **CVE ID : CVE-2021-44143**	https://sourceforge.net/p/isync/isync/commit_browser	A-ISY-ISYN-061221/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Kaspersky					
password_manager					
Improper Privilege Management	23-Nov-21	4.6	A component in Kaspersky Password Manager could allow an attacker to elevate a process Integrity level from Medium to High. **CVE ID : CVE-2021-35052**	https://support.kaspersky.com/general/vulnerability.aspx?el=12430#221121	A-KAS-PASS-061221/263
kazencoders					
url_shortify					
Cross-Site Request Forgery (CSRF)	29-Nov-21	4.3	The URL Shortify WordPress plugin before 1.5.1 does not have CSRF check in place when bulk-deleting links or groups, which could allow attackers to make a logged in admin delete arbitrary link and group via a CSRF attack. **CVE ID : CVE-2021-24749**	N/A	A-KAZ-URL_-061221/264
kimai					
kimai_2					
Cross-Site Request Forgery (CSRF)	19-Nov-21	4.3	kimai2 is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-3957**	https://github.com/kevinpapst/kimai2/commit/6b49535b523dcd36ec59462ee4e67e2b3a9151f3, https://hunt r.dev/bounties/5fa3098a-ba02-45e0-af56-645e34dbc691	A-KIM-KIMA-061221/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	19-Nov-21	4.3	kimai2 is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-3963**	https://hunt r.dev/bounti es/3abf308b -7dbd-4864-b1a9-5c45b876de f8, https://gith ub.com/kevi npapst/kima i2/commit/ 95796ab256 0ad93f4406 8a88f0fad75 8c2053514	A-KIM-KIMA-061221/266
Cross-Site Request Forgery (CSRF)	19-Nov-21	4.3	kimai2 is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-3976**	https://gith ub.com/kevi npapst/kima i2/commit/ b28e9c120c 87222e21a2 38f1b03a60 9d6a5d506e , https://hunt r.dev/bounti es/0567048 a-118c-42ec-9f94-b555330174 06	A-KIM-KIMA-061221/267
librecad					
libdxfrw					
Out-of-bounds Write	19-Nov-21	6.8	A code execution vulnerability exists in the dwgCompressor::decompress 18() functionality of LibreCad libdxfrw 2.2.0-rc2-19-ge02f3580. A specially-crafted .dwg file can lead to an out-of-	N/A	A-LIB-LIBD-061221/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bounds write. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21898**		
Out-of-bounds Write	19-Nov-21	6.8	A code execution vulnerability exists in the dwgCompressor::copyCompBytes21 functionality of LibreCad libdxfrw 2.2.0-rc2-19-ge02f3580. A specially-crafted .dwg file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21899**	N/A	A-LIB-LIBD-061221/269
Use After Free	19-Nov-21	6.8	A code execution vulnerability exists in the dxfRW::processLType() functionality of LibreCad libdxfrw 2.2.0-rc2-19-ge02f3580. A specially-crafted .dxf file can lead to a use-after-free vulnerability. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21900**	N/A	A-LIB-LIBD-061221/270
Linuxfoundation					
auth_backend					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Nov-21	4.3	Backstage is an open platform for building developer portals. In affected versions the auth-backend plugin allows a malicious actor to trick another user into visiting a vulnerable URL that executes an XSS attack. This attack can	https://github.com/backstage/backstage/security/advisories/GHSA-w7fj-336r-vw49	A-LIN-AUTH-061221/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially allow the attacker to exfiltrate access tokens or other secrets from the user's browser. The default CSP does prevent this attack, but it is expected that some deployments have these policies disabled due to incompatibilities. This is vulnerability is patched in version `0.4.9` of `@backstage/plugin-auth-backend`. **CVE ID : CVE-2021-43776**		
fabric					
NULL Pointer Dereference	18-Nov-21	5	A vulnerability has been detected in HyperLedger Fabric v1.4.0, v2.0.0, v2.1.0. This bug can be leveraged by constructing a message whose payload is nil and sending this message with the method 'forwardToLeader'. This bug has been admitted and fixed by the developers of Fabric. If leveraged, any leader node will crash. **CVE ID : CVE-2021-43667**	https://jira.hyperledger.org/browse/FAB-18529, https://github.com/hyperledger/fabric/pull/2844	A-LIN-FABR-061221/272
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	18-Nov-21	5	A vulnerability has been detected in HyperLedger Fabric v1.4.0, v2.0.0, v2.0.1, v2.3.0. It can easily break down as many orderers as the attacker wants. This bug can be leveraged by constructing a message whose header is invalid to the interface Order. This bug has been admitted and fixed by the developers of	https://jira.hyperledger.org/browse/FAB-18528, https://github.com/hyperledger/fabric/pull/2828	A-LIN-FABR-061221/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Fabric. **CVE ID : CVE-2021-43669**		
open_container_initiative_distribution_specification					
Access of Resource Using Incompatible Type ('Type Confusion')	17-Nov-21	4	The OCI Distribution Spec project defines an API protocol to facilitate and standardize the distribution of content. In the OCI Distribution Specification version 1.0.0 and prior, the Content-Type header alone was used to determine the type of document during push and pull operations. Documents that contain both "manifests" and "layers" fields could be interpreted as either a manifest or an index in the absence of an accompanying Content-Type header. If a Content-Type header changed between two pulls of the same digest, a client may interpret the resulting content differently. The OCI Distribution Specification has been updated to require that a mediaType value present in a manifest or index match the Content-Type header used during the push and pull operations. Clients pulling from a registry may distrust the Content-Type header and reject an ambiguous document that contains both "manifests" and "layers" fields or "manifests" and "config" fields if they are unable to update to version 1.0.1 of the	https://github.com/opencontainers/distribution-spec/security/advisories/GHSA-mc8v-mgrf-8f4m, https://github.com/opencontainers/distribution-spec/commit/ac28cac0557bcd3084714ab09f9f2356fe504923	A-LIN-OPEN-061221/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			spec. **CVE ID : CVE-2021-41190**		
open_container_initiative_image_format_specification					
Access of Resource Using Incompatible Type ('Type Confusion')	17-Nov-21	4	The OCI Distribution Spec project defines an API protocol to facilitate and standardize the distribution of content. In the OCI Distribution Specification version 1.0.0 and prior, the Content-Type header alone was used to determine the type of document during push and pull operations. Documents that contain both "manifests" and "layers" fields could be interpreted as either a manifest or an index in the absence of an accompanying Content-Type header. If a Content-Type header changed between two pulls of the same digest, a client may interpret the resulting content differently. The OCI Distribution Specification has been updated to require that a mediaType value present in a manifest or index match the Content-Type header used during the push and pull operations. Clients pulling from a registry may distrust the Content-Type header and reject an ambiguous document that contains both "manifests" and "layers" fields or "manifests" and "config" fields if they are unable to update to version 1.0.1 of the	https://github.com/opencontainers/distribution-spec/security/advisories/GHSA-mc8v-mgrf-8f4m, https://github.com/opencontainers/distribution-spec/commit/ac28cac0557bcd3084714ab09f9f2356fe504923	A-LIN-OPEN-061221/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			spec. **CVE ID : CVE-2021-41190**		
mainwp					
mainwp_child					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Nov-21	6	The MainWP Child WordPress plugin before 4.1.8 does not validate the orderby and order parameter before using them in a SQL statement, leading to an SQL injection exploitable by high privilege users such as admin when the Backup and Staging by WP Time Capsule plugin is installed **CVE ID : CVE-2021-24877**	N/A	A-MAI-MAIN-061221/276
mandsconsulting					
email_before_download					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Nov-21	6.5	The Email Before Download WordPress plugin before 6.8 does not properly validate and escape the order and orderby GET parameters before using them in SQL statements, leading to authenticated SQL injection issues **CVE ID : CVE-2021-24748**	N/A	A-MAN-EMAI-061221/277
Matrix					
synapse					
Improper Limitation of a Pathname to a Restricted Directory ('Path	23-Nov-21	4.3	Synapse is a package for Matrix homeservers written in Python 3/Twisted. Prior to version 1.47.1, Synapse instances with the media repository enabled can be tricked into downloading a	https://github.com/matrix-org/synapse/security/advisories/GHSA-3hfw-	A-MAT-SYNA-061221/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			file from a remote server into an arbitrary directory. No authentication is required for the affected endpoint. The last 2 directories and file name of the path are chosen randomly by Synapse and cannot be controlled by an attacker, which limits the impact. Homeservers with the media repository disabled are unaffected. Homeservers with a federation whitelist are also unaffected, since Synapse will check the remote hostname, including the trailing `../`s, against the whitelist. Server administrators should upgrade to 1.47.1 or later. Server administrators using a reverse proxy could, at the expense of losing media functionality, may block the certain endpoints as a workaround. Alternatively, non-containerized deployments can be adapted to use the hardened systemd config. **CVE ID : CVE-2021-41281**	x7gx-437c, https://github.com/matrix-org/synapse/commit/91f2bd090	
Mcafee					
policy_auditor					
Improper Neutralization of Input During Web Page Generation ('Cross-site	23-Nov-21	4.3	A Reflected Cross-Site Scripting vulnerability in McAfee Policy Auditor prior to 6.5.2 allows a remote unauthenticated attacker to inject arbitrary web script or HTML via the profileNodeID request parameters. The	https://kc.mcafee.com/corporate/index?page=content&id=SB10372	A-MCA-POLI-061221/279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			malicious script is reflected unmodified into the Policy Auditor web-based interface which could lead to the extraction of end user session token or login credentials. These may be used to access additional security-critical applications or conduct arbitrary cross-domain requests. **CVE ID : CVE-2021-31851**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	4.3	A Reflected Cross-Site Scripting vulnerability in McAfee Policy Auditor prior to 6.5.2 allows a remote unauthenticated attacker to inject arbitrary web script or HTML via the UID request parameter. The malicious script is reflected unmodified into the Policy Auditor web-based interface which could lead to the extract of end user session token or login credentials. These may be used to access additional security-critical applications or conduct arbitrary cross-domain requests. **CVE ID : CVE-2021-31852**	https://kc.mcafee.com/corporate/index?page=content&id=SB10372	A-MCA-POLI-061221/280
meddata					
hbys					
Improper Neutralization of Special Elements used in an SQL	16-Nov-21	7.5	Due to improper sanitization MedData HBYS software suffers from a remote SQL injection vulnerability. An unauthenticated attacker with the web access is able to	https://github.com/bartutku/CVE-2021-43361/blob/main/CVE-	A-MED-HBYS-061221/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			extract critical information from the system. **CVE ID : CVE-2021-43361**	2021-43361.txt	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Nov-21	7.5	Due to improper sanitization MedData HBYS software suffers from a remote SQL injection vulnerability. An unauthenticated attacker with the web access is able to extract critical information from the system. **CVE ID : CVE-2021-43362**	https://gist.github.com/Blackh4n/9d8feaf1cfb68f66de17361e85f616d4	A-MED-HBYS-061221/282
media-tags_project					
media-tags					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	The Media-Tags WordPress plugin through 3.2.0.2 does not sanitise and escape any of its Labels settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_htnl capability is disallowed. **CVE ID : CVE-2021-24899**	N/A	A-MED-MEDI-061221/283
meetecho					
janus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Nov-21	3.5	janus-gateway is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-4020**	https://hunt r.dev/bounti es/9814baa8-7bdd-4e31-a132-d9d15653409e, https://gith ub.com/mee	A-MEE-JANU-061221/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				techo/janus-gateway/commit/d3fc00ec803d6c41d8f98908732f44e7f4911a1c	
mercari					
mercari					
Incorrect Authorization	24-Nov-21	5	Improper authorization in handler for custom URL scheme vulnerability in Android App 'Mercari (Merpay) - Marketplace and Mobile Payments App' (Japan version) versions prior to 4.49.1 allows a remote attacker to lead a user to access an arbitrary website and the website launches an arbitrary Activity of the app via the vulnerable App, which may result in Mercari account's access token being obtained. **CVE ID : CVE-2021-20835**	N/A	A-MER-MERC-061221/285
metabase					
metabase					
Improper Input Validation	17-Nov-21	5	Metabase is an open source data analytics platform. In affected versions a security issue has been discovered with the custom GeoJSON map (`admin->settings->maps->custom maps->add a map`) support and potential local file inclusion (including environment variables). URLs were not validated prior to	https://github.com/metabase/metabase/commit/042a36e49574c749f944e19cf80360fd3dc322f0, https://github.com/met	A-MET-META-061221/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			being loaded. This issue is fixed in a new maintenance release (0.40.5 and 1.40.5), and any subsequent release after that. If youâ€™re unable to upgrade immediately, you can mitigate this by including rules in your reverse proxy or load balancer or WAF to provide a validation filter before the application. **CVE ID : CVE-2021-41277**	abase/metabase/security/advisories/GHSA-w73v-6p7p-fpfr	
metagauss					
download_plugin					
Incorrect Permission Assignment for Critical Resource	23-Nov-21	3.5	The Download Plugin WordPress plugin before 1.6.1 does not have capability and CSRF checks in the dpwap_plugin_activate AJAX action, allowing any authenticated users, such as subscribers, to activate plugins that are already installed. **CVE ID : CVE-2021-24703**	N/A	A-MET-DOWN-061221/287
Microsoft					
azure_active_directory					
Exposure of Resource to Wrong Sphere	24-Nov-21	4	Azure Active Directory Information Disclosure Vulnerability **CVE ID : CVE-2021-42306**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42306	A-MIC-AZUR-061221/288
azure_active_site_recovery					
Exposure of Resource to	24-Nov-21	4	Azure Active Directory Information Disclosure	https://portal.msrc.micr	A-MIC-AZUR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			Vulnerability **CVE ID : CVE-2021-42306**	osoft.com/en-US/security-guidance/advisory/CVE-2021-42306	061221/289
azure_automation					
Exposure of Resource to Wrong Sphere	24-Nov-21	4	Azure Active Directory Information Disclosure Vulnerability **CVE ID : CVE-2021-42306**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42306	A-MIC-AZUR-061221/290
azure_migrate					
Exposure of Resource to Wrong Sphere	24-Nov-21	4	Azure Active Directory Information Disclosure Vulnerability **CVE ID : CVE-2021-42306**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42306	A-MIC-AZUR-061221/291
clarity					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Nov-21	3.5	There is a Cross-Site Scripting vulnerability in Microsoft Clarity version 0.3. The XSS payload executes whenever the user changes the clarity configuration in Microsoft Clarity version 0.3. The payload is stored on the configuring project Id page. **CVE ID : CVE-2021-33850**	N/A	A-MIC-CLAR-061221/292
edge_chromium					
Authentication Bypass by	24-Nov-21	5	Microsoft Edge (Chromium-based) Spoofing Vulnerability	https://portal.msrc.micr	A-MIC-EDGE-061221/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Spoofing			**CVE ID : CVE-2021-42308**	osoft.com/en-US/security-guidance/advisory/CVE-2021-42308	
Improper Control of Generation of Code ('Code Injection')	24-Nov-21	4	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability **CVE ID : CVE-2021-43221**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43221	A-MIC-EDGE-061221/294
edge_ios					
Authentication Bypass by Spoofing	24-Nov-21	5	Microsoft Edge for iOS Spoofing Vulnerability **CVE ID : CVE-2021-43220**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43220	A-MIC-EDGE-061221/295
windows_10_update_assistant					
Improper Link Resolution Before File Access ('Link Following')	24-Nov-21	6.9	Windows 10 Update Assistant Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-43211. **CVE ID : CVE-2021-42297**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42297	A-MIC-WIND-061221/296
Improper Privilege Management	24-Nov-21	6.6	Windows 10 Update Assistant Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42297. **CVE ID : CVE-2021-43211**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	A-MIC-WIND-061221/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-43211	
Mitsubishielectric					
gt_softgot2000					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	A-MIT-GT_S-061221/298
moddable					
moddable					
Out-of-bounds Write	19-Nov-21	4.3	OpenSource Moddable v10.5.0 was discovered to contain a heap buffer overflow via the component /modules/network/wifi/esp/modwifi.c. **CVE ID : CVE-2021-29323**	https://github.com/Moddable-OpenSource/moddable/issues/5	A-MOD-MODD-061221/299
Out-of-bounds Write	19-Nov-21	6.8	OpenSource Moddable v10.5.0 was discovered to contain a stack overflow via the component /moddable/xs/sources/xsScri	N/A	A-MOD-MODD-061221/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pt.c. **CVE ID : CVE-2021-29324**		
Out-of-bounds Write	19-Nov-21	6.8	OpenSource Moddable v10.5.0 was discovered to contain a heap buffer overflow in the fx_String_prototype_repeat function at /moddable/xs/sources/xsString.c. **CVE ID : CVE-2021-29325**	https://github.com/Moddable-OpenSource/moddable/issues/582	A-MOD-MODD-061221/301
Out-of-bounds Write	19-Nov-21	6.8	OpenSource Moddable v10.5.0 was discovered to contain a heap buffer overflow in the fxIDToString function at /moddable/xs/sources/xsSymbol.c. **CVE ID : CVE-2021-29326**	N/A	A-MOD-MODD-061221/302
Out-of-bounds Write	19-Nov-21	6.8	OpenSource Moddable v10.5.0 was discovered to contain a heap buffer overflow in the fx_ArrayBuffer function at /moddable/xs/sources/xsDataView.c. **CVE ID : CVE-2021-29327**	N/A	A-MOD-MODD-061221/303
Out-of-bounds Read	19-Nov-21	5.8	OpenSource Moddable v10.5.0 was discovered to contain buffer over-read in the fxDebugThrow function at /moddable/xs/sources/xsDebug.c. **CVE ID : CVE-2021-29328**	https://github.com/Moddable-OpenSource/moddable/issues/585	A-MOD-MODD-061221/304
Out-of-bounds Write	19-Nov-21	6.8	OpenSource Moddable v10.5.0 was discovered to contain a stack overflow in the	https://github.com/Moddable-OpenSource	A-MOD-MODD-061221/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fxBinaryExpressionNodeDistribute function at /moddable/xs/sources/xsTree.c. **CVE ID : CVE-2021-29329**	/moddable/issues/587	
Mongodb					
mongodb					
Reachable Assertion	24-Nov-21	4	An authorized user may trigger an invariant which may result in denial of service or server exit if a relevant aggregation request is sent to a shard. Usually, the requests are sent via mongos and special privileges are required in order to know the address of the shards and to log in to the shards of an auth enabled environment. **CVE ID : CVE-2021-32037**	https://jira.mongodb.org/browse/SERVER-59071	A-MON-MONG-061221/306
Moodle					
moodle					
Improper Input Validation	22-Nov-21	7.5	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. A remote code execution risk when restoring backup files was identified. **CVE ID : CVE-2021-3943**	https://moodle.org/mod/forum/discuss.php?d=429095	A-MOO-MOOD-061221/307
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-21	4.3	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. A URL parameter in the filetype site administrator tool required extra sanitizing to prevent a reflected XSS	https://moodle.org/mod/forum/discuss.php?d=429097	A-MOO-MOOD-061221/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			risk. **CVE ID : CVE-2021-43558**		
Cross-Site Request Forgery (CSRF)	22-Nov-21	6.8	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. The "delete related badge" functionality did not include the necessary token check to prevent a CSRF risk. **CVE ID : CVE-2021-43559**	https://moodle.org/mod/forum/discuss.php?d=429099	A-MOO-MOOD-061221/309
Exposure of Resource to Wrong Sphere	22-Nov-21	5	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. Insufficient capability checks made it possible to fetch other users' calendar action events. **CVE ID : CVE-2021-43560**	https://moodle.org/mod/forum/discuss.php?d=429100	A-MOO-MOOD-061221/310
mousewheel_smooth_scroll_project					
mousewheel_smooth_scroll					
Cross-Site Request Forgery (CSRF)	17-Nov-21	4.3	The MouseWheel Smooth Scroll WordPress plugin before 5.7 does not have CSRF check in place on its settings page, which could allow attackers to make a logged in admin change them via a CSRF attack **CVE ID : CVE-2021-24852**	N/A	A-MOU-MOUS-061221/311
mycred					
mycred					
Improper Neutralization of Special Elements used in an	29-Nov-21	6.5	The myCred WordPress plugin before 2.3 does not validate or escape the fields parameter before using it in a SQL statement, leading to an	N/A	A-MYC-MYCR-061221/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			SQL injection exploitable by any authenticated user **CVE ID : CVE-2021-24755**		
myscada					
mydesigner					
Relative Path Traversal	19-Nov-21	6.8	mySCADA myDESIGNER Versions 8.20.0 and prior fails to properly validate contents of an imported project file, which may make the product vulnerable to a path traversal payload. This vulnerability may allow an attacker to plant files on the file system in arbitrary locations or overwrite existing files, resulting in remote code execution. **CVE ID : CVE-2021-43555**	https://us-cert.cisa.gov/ics/advisories/icsa-21-313-04	A-MYS-MYDE-061221/313
my_calendar_project					
my_calendar					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	The My Calendar WordPress plugin before 3.2.18 does not sanitise and escape the callback parameter of the mc_post_lookup AJAX action (available to any authenticated user) before outputting it back in the response, leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24927**	N/A	A-MY_-MY_C-061221/314
my_tickets_project					
my_tickets					
Improper	17-Nov-21	4.3	The My Tickets WordPress	N/A	A-MY_-MY_T-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			plugin before 1.8.31 does not properly sanitise and escape the Email field of booked tickets before outputting it in the Payment admin dashboard, which could allow unauthenticated users to perform Cross-Site Scripting attacks against admins **CVE ID : CVE-2021-24796**		061221/315
nebulab					
solidus_auth_devise					
Cross-Site Request Forgery (CSRF)	17-Nov-21	6.8	solidus_auth_devise provides authentication services for the Solidus webstore framework, using the Devise gem. In affected versions solidus_auth_devise is subject to a CSRF vulnerability that allows user account takeover. All applications using any version of the frontend component of `solidus_auth_devise` are affected if `protect_from_forgery` method is both: Executed whether as: A `before_action` callback (the default) or A `prepend_before_action` (option `prepend: true` given) before the `:load_object` hook in `Spree::UserController` (most likely order to find). Configured to use `:null_session` or `:reset_session` strategies (`:null_session` is the default in case the no strategy is given, but `rails --new`	https://github.com/solidusio/solidus_auth_devise/security/advisories/GHSA-xm34-v85h-9pg2, https://github.com/solidusio/solidus_auth_devise/commit/731a6645e90ea9fd228f78ec53c6976c048a0555	A-NEB-SOLI-061221/316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			generated skeleton use `:exception`). Users should promptly update to `solidus_auth_devise` version `2.5.4`. Users unable to update should if possible, change their strategy to `:exception`. Please see the linked GHSA for more workaround details. **CVE ID : CVE-2021-41274**		
Ninjaforms					
ninja_forms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Nov-21	6.5	The Ninja Forms Contact Form WordPress plugin before 3.6.4 does not escape keys of the fields POST parameter, which could allow high privilege users to perform SQL injections attacks **CVE ID : CVE-2021-24889**	N/A	A-NIN-NINJ-061221/317
nodebb					
nodebb					
Improper Authentication	29-Nov-21	5	Nodebb is an open source Node.js based forum software. In affected versions incorrect logic present in the token verification step unintentionally allowed master token access to the API. The vulnerability has been patch as of v1.18.5. Users are advised to upgrade as soon as possible. **CVE ID : CVE-2021-43786**	https://github.com/NodeBB/NodeBB/security/advisories/GHSA-hf2m-j98r-4fqw, https://github.com/NodeBB/NodeBB/commit/04dab1d550cdebf4c1567bca9a51f8b9ca48a500	A-NOD-NODE-061221/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	4.3	Nodebb is an open source Node.js based forum software. In affected versions a prototype pollution vulnerability in the uploader module allowed a malicious user to inject arbitrary data (i.e. javascript) into the DOM, theoretically allowing for an account takeover when used in conjunction with a path traversal vulnerability disclosed at the same time as this report. The vulnerability has been patched as of v1.18.5. Users are advised to upgrade as soon as possible. **CVE ID : CVE-2021-43787**	https://github.com/NodeBB/NodeBB/releases/tag/v1.18.5, https://github.com/NodeBB/NodeBB/commit/1783f918bc19568f421473824461ff2ed7755e4c, https://github.com/NodeBB/NodeBB/security/advisories/GHSA-wx69-rvg3-x7fc	A-NOD-NODE-061221/319
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Nov-21	4	Nodebb is an open source Node.js based forum software. Prior to v1.18.5, a path traversal vulnerability was present that allowed users to access JSON files outside of the expected `languages/` directory. The vulnerability has been patched as of v1.18.5. Users are advised to upgrade as soon as possible. **CVE ID : CVE-2021-43788**	https://github.com/NodeBB/NodeBB/security/advisories/GHSA-pfj7-2qfw-vwgm, https://github.com/NodeBB/NodeBB/commit/c8b2fc46dc698db687379106b3f01c71b80f495f	A-NOD-NODE-061221/320
octopus					
tentacle					
Incorrect Default	24-Nov-21	4.6	When Octopus Tentacle is installed on a Linux operating system, the systemd service	https://advisories.octopus.com/adv/	A-OCT-TENT-061221/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			file permissions are misconfigured. This could lead to a local unprivileged user modifying the contents of the systemd service file to gain privileged access. **CVE ID : CVE-2021-31822**	2021-11---Local-privilege-escalation-in-Octopus-Tentacle-(CVE-2021-31822).2283732993.html	
oisf					
suricata					
Out-of-bounds Write	19-Nov-21	7.5	Suricata before 5.0.8 and 6.x before 6.0.4 allows TCP evasion via a client with a crafted TCP/IP stack that can send a certain sequence of segments. **CVE ID : CVE-2021-37592**	https://forum.suricata.io/t/suricata-6-0-4-and-5-0-8-released/1942, https://redmine.openinfosecfoundation.org/issues/4569	A-OIS-SURI-061221/322
Open-xchange					
ox_app_suite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-21	3.5	OX App Suite through through 7.10.5 allows XSS via a crafted snippet that has an app loader reference within an app loader URL. **CVE ID : CVE-2021-38374**	N/A	A-OPE-OX_A-061221/323
Improper Neutralization of Input During Web Page Generation	22-Nov-21	4.3	OX App Suite through 7.10.5 allows XSS via the alt attribute of an IMG element in a truncated e-mail message. **CVE ID : CVE-2021-38375**	N/A	A-OPE-OX_A-061221/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Exposure of Resource to Wrong Sphere	22-Nov-21	5	OX App Suite through 7.10.5 has Incorrect Access Control for retrieval of session information via the rampup action of the login API call. **CVE ID : CVE-2021-38376**	N/A	A-OPE-OX_A-061221/325
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-21	4.3	OX App Suite through 7.10.5 allows XSS via JavaScript code in an anchor HTML comment within truncated e-mail, because there is a predictable UUID with HTML transformation results. **CVE ID : CVE-2021-38377**	N/A	A-OPE-OX_A-061221/326
Exposure of Resource to Wrong Sphere	22-Nov-21	4	OX App Suite 7.10.5 allows Information Exposure because a caching mechanism can caused a Modified By response to show a person's name. **CVE ID : CVE-2021-38378**	N/A	A-OPE-OX_A-061221/327
Improper Input Validation	22-Nov-21	5.8	chat in OX App Suite 7.10.5 has Improper Input Validation. A user can be redirected to a rogue OX Chat server via a development-related hook. **CVE ID : CVE-2021-33488**	N/A	A-OPE-OX_A-061221/328
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-21	4.3	OX App Suite through 7.10.5 allows XSS via JavaScript code in a shared XCF file. **CVE ID : CVE-2021-33489**	N/A	A-OPE-OX_A-061221/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-21	4.3	OX App Suite through 7.10.5 allows XSS via a crafted snippet in a shared mail signature. **CVE ID : CVE-2021-33490**	N/A	A-OPE-OX_A-061221/330
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Nov-21	4	OX App Suite through 7.10.5 allows Directory Traversal via ../ in an OOXML or ODF ZIP archive, because of the mishandling of relative paths in mail addresses in conjunction with auto-configuration DNS records. **CVE ID : CVE-2021-33491**	https://open-xchange.com	A-OPE-OX_A-061221/331
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-21	4.3	OX App Suite 7.10.5 allows XSS via an OX Chat room name. **CVE ID : CVE-2021-33492**	https://open-xchange.com	A-OPE-OX_A-061221/332
Improper Control of Generation of Code ('Code Injection')	22-Nov-21	3.6	The middleware component in OX App Suite through 7.10.5 allows Code Injection via Java classes in a YAML format. **CVE ID : CVE-2021-33493**	https://open-xchange.com	A-OPE-OX_A-061221/333
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-21	4.3	OX App Suite 7.10.5 allows XSS via an OX Chat room title during typing rendering. **CVE ID : CVE-2021-33494**	https://open-xchange.com	A-OPE-OX_A-061221/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-21	4.3	OX App Suite 7.10.5 allows XSS via an OX Chat system message. **CVE ID : CVE-2021-33495**	N/A	A-OPE-OX_A-061221/335
opendesign					
drawings_sdk					
Use After Free	22-Nov-21	6.8	A Use-After-Free Remote Vulnerability exists when reading a DWG file using Open Design Alliance Drawings SDK before 2022.11. The specific issue exists within the parsing of DWG files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2021-43582**	https://www.opendesign.com/security-advisories	A-OPE-DRAW-061221/336
prc_sdk					
Out-of-bounds Read	22-Nov-21	6.8	An Out-of-Bounds Read vulnerability exists when reading a U3D file using Open Design Alliance PRC SDK before 2022.11. The specific issue exists within the parsing of U3D files. Incorrect use of the LibJpeg source manager inside the U3D library, and crafted data in a U3D file, can trigger a read past the end of an allocated buffer. An attacker can leverage this	https://www.opendesign.com/security-advisories	A-OPE-PRC_-061221/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to execute code in the context of the current process. **CVE ID : CVE-2021-43581**		
openpolicyagent					
gatekeeper					
Improper Handling of Exceptional Conditions	17-Nov-21	5	** DISPUTED ** Styra Open Policy Agent (OPA) Gatekeeper through 3.7.0 mishandles concurrency, sometimes resulting in incorrect access control. The data replication mechanism allows policies to access the Kubernetes cluster state. During data replication, OPA/Gatekeeper does not wait for the replication to finish before processing a request, which might cause inconsistencies between the replicated resources in OPA/Gatekeeper and the resources actually present in the cluster. Inconsistency can later be reflected in a policy bypass. NOTE: the vendor disagrees that this is a vulnerability, because Kubernetes states are only eventually consistent. **CVE ID : CVE-2021-43979**	https://github.com/open-policy-agent/gatekeeper/releases	A-OPE-GATE-061221/338
optical_character_recognition_project					
optical_character_recognition					
Out-of-bounds Write	17-Nov-21	6.8	A stack-based buffer overflow vulnerability was discovered in gocr through 0.53-20200802 in measure_pitch()	N/A	A-OPT-OPTI-061221/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in pgm2asc.c. **CVE ID : CVE-2021-33479**		
Use After Free	17-Nov-21	4.3	An use-after-free vulnerability was discovered in gocr through 0.53-20200802 in context_correction() in pgm2asc.c. **CVE ID : CVE-2021-33480**	N/A	A-OPT-OPTI-061221/340
Out-of-bounds Write	17-Nov-21	6.8	A stack-based buffer overflow vulnerability was discovered in gocr through 0.53-20200802 in try_to_divide_boxes() in pgm2asc.c. **CVE ID : CVE-2021-33481**	N/A	A-OPT-OPTI-061221/341
oroinc					
client_relationship_management					
Cross-Site Request Forgery (CSRF)	19-Nov-21	5.8	OroCRM is an open source Client Relationship Management (CRM) application. Affected versions we found to suffer from a vulnerability which could an attacker is able to disqualify any Lead with a Cross-Site Request Forgery (CSRF) attack. There are no workarounds that address this vulnerability and all users are advised to update their package. **CVE ID : CVE-2021-39198**	https://github.com/oroinc/crm/security/advisories/GHSA-vf7h-6246-hm43	A-ORO-CLIE-061221/342
os4ed					
opensis					
Improper Neutralization of Special	30-Nov-21	6.8	A SQL injection vulnerability exists in version 8.0 of openSIS when MySQL or	N/A	A-OS4-OPEN-061221/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			MariaDB is used as the application database. An attacker can then issue the SQL command through the /opensis/functions/GetStuListFnc.php &Grade= parameter. **CVE ID : CVE-2021-41677**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-Nov-21	6.8	A SQL injection vulnerability exists in version 8.0 of openSIS when MySQL or MariaDB is used as the application database. An attacker can then issue the SQL command through the /opensis/modules/users/Staff.php, staff{TITLE] parameter. **CVE ID : CVE-2021-41678**	N/A	A-OS4-OPEN-061221/344
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-Nov-21	6.8	A SQL injection vulnerability exists in version 8.0 of openSIS when MySQL or MariaDB is used as the application database. An attacker can then issue the SQL command through the /opensis/modules/grades/InputFinalGrades.php, period parameter. **CVE ID : CVE-2021-41679**	N/A	A-OS4-OPEN-061221/345
Osisoft					
pi_vision					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	3.5	A remote attacker with write access to PI Vision could inject code into a display. Unauthorized information disclosure, modification, or deletion is possible if a victim views or interacts with the infected display using	N/A	A-OSI-PI_V-061221/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Internet Explorer. The impact affects PI System data and other data accessible with victim's user permissions. **CVE ID : CVE-2021-43551**		
Incorrect Authorization	17-Nov-21	4	PI Vision could disclose information to a user with insufficient privileges for an AF attribute that is the child of another attribute and is configured as a Limits property. **CVE ID : CVE-2021-43553**	N/A	A-OSI-PI_V-061221/347
pi_web_api					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-21	3.5	A remote authenticated attacker with write access to a PI Server could trick a user into interacting with a PI Web API endpoint and redirect them to a malicious website. As a result, a victim may disclose sensitive information to the attacker or be provided with false information. **CVE ID : CVE-2021-43549**	N/A	A-OSI-PI_W-061221/348
pekeupload_project					
pekeupload					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-21	4.3	This affects all versions of package pekeupload. If an attacker induces a user to upload a file whose name contains javascript code, the javascript code will be executed. **CVE ID : CVE-2021-23673**	https://github.com/moxiecode/plupload/blob/120cc0b5dd3373d7181fd11b06ac2557c890d3f0/js/jquery.plupload.queue/j	A-PEK-PEKE-061221/349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				query.plupload.queue.js%23L226, https://snyk.io/vuln/SNYK-JS-PEKEUPLOAD-1584360	
pgbouncer					
pgbouncer					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Nov-21	5.1	When PgBouncer is configured to use "cert" authentication, a man-in-the-middle attacker can inject arbitrary SQL queries when a connection is first established, despite the use of TLS certificate verification and encryption. This flaw affects PgBouncer versions prior to 1.16.1. **CVE ID : CVE-2021-3935**	http://www.pgbouncer.org/changelog.html#pgbouncer-116x	A-PGB-PGBO-061221/350
PHP					
php					
N/A	29-Nov-21	5	In PHP versions 7.3.x below 7.3.33, 7.4.x below 7.4.26 and 8.0.x below 8.0.13, certain XML parsing functions, like simplexml_load_file(), URL-decode the filename passed to them. If that filename contains URL-encoded NUL character, this may cause the function to interpret this as the end of the filename, thus interpreting the filename differently from what the user intended, which may lead it to reading a	https://bugs.php.net/bug.php?id=79971	A-PHP-PHP-061221/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			different file than intended. **CVE ID : CVE-2021-21707**		
phpwhois_project					
phpwhois					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	4.3	An unspecified version of phpWhois is affected by a Cross Site Scripting (XSS) vulnerability. In file example.php, the exit function will terminate the script and print the message to the user. The message will contain $_GET['query'] then there is a XSS vulnerability. **CVE ID : CVE-2021-43698**	N/A	A-PHP-PHPW-061221/352
planetargon					
oh_my_zsh					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Nov-21	6.8	Vulnerability in dirhistory plugin Description: the widgets that go back and forward in the directory history, triggered by pressing Alt-Left and Alt-Right, use functions that unsafely execute eval on directory names. If you cd into a directory with a carefully-crafted name, then press Alt-Left, the system is subject to command injection. Impacted areas: - Functions pop_past and pop_future in dirhistory plugin. **CVE ID : CVE-2021-3725**	https://github.com/ohmyzsh/ohmyzsh/commit/06fc5fb	A-PLA-OH_M-061221/353
Improper Neutralization of Special Elements	30-Nov-21	7.5	# Vulnerability in `title` function **Description**: the `title` function defined in `lib/termsupport.zsh` uses	https://github.com/ohmyzsh/ohmyzsh/commit/	A-PLA-OH_M-061221/354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			`print` to set the terminal title to a user-supplied string. In Oh My Zsh, this function is always used securely, but custom user code could use the `title` function in a way that is unsafe. **Fixed in**: [a263cdac](https://github.com/ohmyzsh/ohmyzsh/commit/a263cdac). **Impacted areas**: - `title` function in `lib/termsupport.zsh`. - Custom user code using the `title` function. **CVE ID : CVE-2021-3726**	a263cdac	
preview_e-mails_for_woocommerce_project					
preview_e-mails_for_woocommerce					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Nov-21	4.3	The Preview E-Mails for WooCommerce WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the search_order parameter found in the ~/views/form.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.6.8. **CVE ID : CVE-2021-42363**	https://plugins.trac.wordpress.org/changeset/2625941/woo-preview-emails/trunk/views/form.php	A-PRE-PREV-061221/355
pterodactyl					
panel					
Cross-Site Request Forgery (CSRF)	17-Nov-21	4.3	Pterodactyl is an open-source game server management panel built with PHP 7, React, and Go. Due to improperly configured CSRF protections on two routes, a malicious user could execute a CSRF-	https://github.com/pterodactyl/panel/security/advisories/GHSA-wwgq-9jhf-qgw6,	A-PTE-PANE-061221/356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			based attack against the following endpoints: Sending a test email and Generating a node auto-deployment token. At no point would any data be exposed to the malicious user, this would simply trigger email spam to an administrative user, or generate a single auto-deployment token unexpectedly. This token is not revealed to the malicious user, it is simply created unexpectedly in the system. This has been addressed in release `1.6.6`. Users may optionally manually apply the fixes released in v1.6.6 to patch their own systems. **CVE ID : CVE-2021-41273**	https://github.com/pterodactyl/panel/commit/bf9cbe2c6d5266c6914223e067c56175de7fc3a5	
Pulsesecure					
pulse_connect_secure					
Uncontrolled Resource Consumption	19-Nov-21	7.8	A vulnerability in Pulse Connect Secure before 9.1R12.1 could allow an unauthenticated administrator to causes a denial of service when a malformed request is sent to the device. **CVE ID : CVE-2021-22965**	https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44879/?kA13Z000000L3ZF	A-PUL-PULS-061221/357
Puppet					
continuous_delivery					
Incorrect Permission Assignment for Critical	18-Nov-21	5.5	A flaw was discovered in Continuous Delivery for Puppet Enterprise (CD4PE) that results in a user with	https://puppet.com/security/cve/cve-2021-	A-PUP-CONT-061221/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource			lower privileges being able to access a Puppet Enterprise API token. This issue is resolved in CD4PE 4.10.0 **CVE ID : CVE-2021-27024**	27024	
puppet					
N/A	18-Nov-21	5	A flaw was discovered in Puppet Agent and Puppet Server that may result in a leak of HTTP credentials when following HTTP redirects to a different host. This is similar to CVE-2018-1000007 **CVE ID : CVE-2021-27023**	https://puppet.com/security/cve/CVE-2021-27023	A-PUP-PUPP-061221/359
N/A	18-Nov-21	4	A flaw was discovered in Puppet Agent where the agent may silently ignore Augeas settings or may be vulnerable to a Denial of Service condition prior to the first 'pluginsync'. **CVE ID : CVE-2021-27025**	https://puppet.com/security/cve/cve-2021-27025	A-PUP-PUPP-061221/360
Insertion of Sensitive Information into Log File	18-Nov-21	2.1	A flaw was divered in Puppet Enterprise and other Puppet products where sensitive plan parameters may be logged **CVE ID : CVE-2021-27026**	https://puppet.com/security/cve/cve-2021-27026	A-PUP-PUPP-061221/361
puppet_agent					
N/A	18-Nov-21	5	A flaw was discovered in Puppet Agent and Puppet Server that may result in a leak of HTTP credentials when following HTTP redirects to a different host. This is similar to CVE-2018-1000007	https://puppet.com/security/cve/CVE-2021-27023	A-PUP-PUPP-061221/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27023		
N/A	18-Nov-21	4	A flaw was discovered in Puppet Agent where the agent may silently ignore Augeas settings or may be vulnerable to a Denial of Service condition prior to the first 'pluginsync'. **CVE ID : CVE-2021-27025**	https://puppet.com/security/cve/cve-2021-27025	A-PUP-PUPP-061221/363
puppet_connect					
Insertion of Sensitive Information into Log File	18-Nov-21	2.1	A flaw was divered in Puppet Enterprise and other Puppet products where sensitive plan parameters may be logged **CVE ID : CVE-2021-27026**	https://puppet.com/security/cve/cve-2021-27026	A-PUP-PUPP-061221/364
puppet_server					
N/A	18-Nov-21	5	A flaw was discovered in Puppet Agent and Puppet Server that may result in a leak of HTTP credentials when following HTTP redirects to a different host. This is similar to CVE-2018-1000007 **CVE ID : CVE-2021-27023**	https://puppet.com/security/cve/CVE-2021-27023	A-PUP-PUPP-061221/365
Qnap					
qmailagent					
Cross-Site Request Forgery (CSRF)	20-Nov-21	6.8	We have already fixed this vulnerability in the following versions of QmailAgent: QmailAgent 3.0.2 (2021/08/25) and later **CVE ID : CVE-2021-34358**	https://www.qnap.com/en/security-advisory/qsa-21-49	A-QNA-QMAI-061221/366
ragic_cloud_db					
Improper Neutralizatio	20-Nov-21	4.3	A reflected cross-site scripting (XSS) vulnerability has been	https://www.qnap.com	A-QNA-RAGI-061221/367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			reported to affect QNAP NAS running Ragic Cloud DB. If exploited, this vulnerability allows remote attackers to inject malicious code. QNAP have already disabled and removed Ragic Cloud DB from the QNAP App Center, pending a security patch from Ragic. **CVE ID : CVE-2021-38681**	/en/security-advisory/qsa-21-48	
qr_redirector_project					
qr_redirector					
Cross-Site Request Forgery (CSRF)	17-Nov-21	4.3	The QR Redirector WordPress plugin before 1.6 does not have capability and CSRF checks when saving bulk QR Redirector settings via the qr_save_bulk AJAX action, which could allow any authenticated user, such as subscriber to change the redirect response status code of arbitrary QR Redirects **CVE ID : CVE-2021-24853**	N/A	A-QR_-QR_R-061221/368
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	3.5	The QR Redirector WordPress plugin before 1.6.1 does not sanitise and escape some of the QR Redirect fields, which could allow users with a role as low as Contributor perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2021-24854**	N/A	A-QR_-QR_R-061221/369
Quagga					
quagga					
Improper Privilege	19-Nov-21	7.2	An issue was discovered in Quagga through 1.2.4. Unsafe	N/A	A-QUA-QUAG-061221/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			chown/chmod operations in the suggested spec file allow users (with control of the non-root-owned directory /etc/quagga) to escalate their privileges to root upon package installation or update. **CVE ID : CVE-2021-44038**		
quobject					
docker-cli-js					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Nov-21	9.3	This affects all versions of package docker-cli-js. If the command parameter of the Docker.command method can at least be partially controlled by a user, they will be in a position to execute any arbitrary OS commands on the host system. **CVE ID : CVE-2021-23732**	https://snyk.io/vuln/SNYK-JS-DOCKERCLIJS-1568516	A-QUO-DOCK-061221/371
recruitment_management_system_project					
recruitment_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Nov-21	7.5	The Company's Recruitment Management System in id=2 of the parameter from view_vacancy app on-page appears to be vulnerable to SQL injection. The payloads 19424269' or '1309'='1309 and 39476597' or '2917'='2923 were each submitted in the id parameter. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe	N/A	A-REC-RECR-061221/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			way. **CVE ID : CVE-2021-41931**		
redash					
redash					
URL Redirection to Untrusted Site ('Open Redirect')	24-Nov-21	5.8	Redash is a package for data visualization and sharing. In Redash version 10.0 and prior, the implementation of Google Login (via OAuth) incorrectly uses the `state` parameter to pass the next URL to redirect the user to after login. The `state` parameter should be used for a Cross-Site Request Forgery (CSRF) token, not a static and easily predicted value. This vulnerability does not affect users who do not use Google Login for their instance of Redash. A patch in the `master` and `release/10.x.x` branches addresses this by replacing `Flask-Oauthlib` with `Authlib` which automatically provides and validates a CSRF token for the state variable. The new implementation stores the next URL on the user session object. As a workaround, one may disable Google Login to mitigate the vulnerability. **CVE ID : CVE-2021-43777**	https://github.com/getredash/redash/security/advisories/GHSA-vhc7-w7r8-8m34, https://github.com/getredash/redash/commit/da696ff7f84787cbf85967460fac52886cbe063e	A-RED-REDA-061221/373
Server-Side Request Forgery (SSRF)	24-Nov-21	6	Redash is a package for data visualization and sharing. In versions 10.0 and priorm the implementation of URL-loading data sources like	https://github.com/getredash/redash/security/advisories/G	A-RED-REDA-061221/374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			JSON, CSV, or Excel is vulnerable to advanced methods of Server Side Request Forgery (SSRF). These vulnerabilities are only exploitable on installations where a URL-loading data source is enabled. As of time of publication, the `master` and `release/10.x.x` branches address this by applying the Advocate library for making http requests instead of the requests library directly. Users should upgrade to version 10.0.1 to receive this patch. There are a few workarounds for mitigating the vulnerability without upgrading. One can disable the vulnerable data sources entirely, by adding the following env variable to one's configuration, making them unavailable inside the webapp. One can switch any data source of certain types (viewable in the GitHub Security Advisory) to be `View Only` for all groups on the Settings > Groups > Data Sources screen. For users unable to update an admin may modify Redash's configuration through environment variables to mitigate this issue. Depending on the version of Redash, an admin may also need to run a CLI command to re-encrypt some fields in the database.	HSA-fcpv-hgq6-87h7, https://github.com/getredash/redash/commit/61bbb5aa7a23a93f2f93710005f71bc972826099	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The `master` and `release/10.x.x` branches as of time of publication have removed the default value for `REDASH_COOKIE_SECRET`. All future releases will also require this to be set explicitly. For existing installations, one will need to ensure that explicit values are set for the `REDASH_COOKIE_SECRET` and `REDASH_SECRET_KEY `variables. **CVE ID : CVE-2021-43780**		
rosariosis					
rosariosis					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Nov-21	7.5	An unauthenticated SQL Injection vulnerability in Rosario Student Information System (aka rosariosis) before 8.1.1 allows remote attackers to execute PostgreSQL statements (e.g., SELECT, INSERT, UPDATE, and DELETE) through /Side.php via the syear parameter. **CVE ID : CVE-2021-44427**	N/A	A-ROS-ROSA-061221/375
Roundcube					
webmail					
Improper Neutralization of Input During Web Page Generation ('Cross-site	19-Nov-21	4.3	Roundcube before 1.3.17 and 1.4.x before 1.4.12 is prone to XSS in handling an attachment's filename extension when displaying a MIME type warning message. **CVE ID : CVE-2021-44025**	https://github.com/roundcube/roundcubemail/commit/7d7b1dfeff795390b69905ce	A-ROU-WEBM-061221/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')				b63d6391b5b0dfe7, https://github.com/roundcube/roundcubemail/issues/8193, https://github.com/roundcube/roundcubemail/commit/faf99bf8a2b7b7562206fa047e8de652861e624a	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Nov-21	7.5	Roundcube before 1.3.17 and 1.4.x before 1.4.12 is prone to a potential SQL injection via search or search_params. **CVE ID : CVE-2021-44026**	https://github.com/roundcube/roundcubemail/commit/ee809bde2dcaa04857a919397808a7296681dcfa, https://github.com/roundcube/roundcubemail/commit/c8947ecb762d9e89c2091bda28d49002817263f1	A-ROU-WEBM-061221/377
roundupwp					
registrations_for_the_events_calendar					
Improper Neutralization of Input During Web	29-Nov-21	4.3	The Registrations for the Events Calendar WordPress plugin before 2.7.5 does not escape the v parameter before	N/A	A-ROU-REGI-061221/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			outputting it back in an attribute, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2021-24876**		
rwtxt_project					
rwtxt					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Nov-21	4.3	Cross-site scripting vulnerability in rwtxt versions prior to v1.8.6 allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20848**	N/A	A-RWT-RWTX-061221/379
s3scanner_project					
s3scanner					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Nov-21	5	S3Scanner before 2.0.2 allows Directory Traversal via a crafted bucket, as demonstrated by a <Key>../ substring in a ListBucketResult element. **CVE ID : CVE-2021-32061**	N/A	A-S3S-S3SC-061221/380
saasproject					
booking_package					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Nov-21	4.3	Cross-site scripting vulnerability in Booking Package - Appointment Booking Calendar System versions prior to 1.5.11 allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20840**	https://saasproject.net/ja/fixed/20211019.php	A-SAA-BOOK-061221/381
SAS					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sas\\/intrnet					
Inclusion of Functionality from Untrusted Control Sphere	19-Nov-21	5	SAS/Intrnet 9.4 build 1520 and earlier allows Local File Inclusion. The samples library (included by default) in the appstart.sas file, allows end-users of the application to access the sample.webcsf1.sas program, which contains user-controlled macro variables that are passed to the DS2CSF macro. Users can escape the context of the configured user-controllable variable and append additional functions native to the macro but not included as variables within the library. This includes a function that retrieves files from the host OS. **CVE ID : CVE-2021-41569**	N/A	A-SAS-SAS\-061221/382
Schedmd					
slurm					
Incorrect Authorization	17-Nov-21	4	SchedMD Slurm 21.08.* before 21.08.4 has Incorrect Access Control. On sites using the new AccountingStoreFlags=job_script and/or job_env options, the access control rules in SlurmDBD may permit users to request job scripts and environment files to which they should not have access. **CVE ID : CVE-2021-43337**	https://lists.schedmd.com/pipermail/slurm-announce/, https://www.schedmd.com/news.php, https://www.schedmd.com/news.php?id=256, https://lists.schedmd.co	A-SCH-SLUR-061221/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				m/pipermail/slurm-announce/2021/000068.html	
Sensiolabs					
symfony					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	24-Nov-21	4.3	Symfony/Http-Kernel is the HTTP kernel component for Symfony, a PHP framework for web and console applications and a set of reusable PHP components. Headers that are not part of the "trusted_headers" allowed list are ignored and protect users from "Cache poisoning" attacks. In Symfony 5.2, maintainers added support for the `X-Forwarded-Prefix` headers, but this header was accessible in SubRequest, even if it was not part of the "trusted_headers" allowed list. An attacker could leverage this opportunity to forge requests containing a `X-Forwarded-Prefix` header, leading to a web cache poisoning issue. Versions 5.3.12 and later have a patch to ensure that the `X-Forwarded-Prefix` header is not forwarded to subrequests when it is not trusted. **CVE ID : CVE-2021-41267**	https://github.com/symfony/symfony/security/advisories/GHSA-q3j3-w37x-hq2q, https://github.com/symfony/symfony/commit/95dcf51682029e89450aee86267e3d553aa7c487, https://github.com/symfony/symfony/pull/44243	A-SEN-SYMF-061221/384
Session Fixation	24-Nov-21	6.5	Symfony/SecurityBundle is the security system for Symfony, a PHP framework	https://github.com/symfony/symfon	A-SEN-SYMF-061221/385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for web and console applications and a set of reusable PHP components. Since the rework of the Remember me cookie in version 5.3.0, the cookie is not invalidated when the user changes their password. Attackers can therefore maintain their access to the account even if the password is changed as long as they have had the chance to login once and get a valid remember me cookie. Starting with version 5.3.12, Symfony makes the password part of the signature by default. In that way, when the password changes, then the cookie is not valid anymore. **CVE ID : CVE-2021-41268**	y/security/advisories/GHSA-qw36-p97w-vcqr, https://github.com/symfony/symfony/commit/36a808b857cd3240244f4b224452fb1e70dc6dfc, https://github.com/symfony/symfony/pull/44243	
sharetribe					
sharetribe					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Nov-21	7.5	Sharetribe Go is a source available marketplace software. In affected versions operating system command injection is possible on installations of Sharetribe Go, that do not have a secret AWS Simple Notification Service (SNS) notification token configured via the `sns_notification_token` configuration parameter. This configuration parameter is unset by default. The vulnerability has been patched in version 10.2.1.	https://github.com/sharetribe/sharetribe/security/advisories/GHSA-hjjc-p9hr-424c, https://github.com/sharetribe/sharetribe/commit/5b844f8108c5458d89f0d7ba974f42d7917b5f8	A-SHA-SHAR-061221/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Users who are unable to upgrade should set the`sns_notification_token` configuration parameter to a secret value. **CVE ID : CVE-2021-41280**	0	
shoppagewp					
shop_page_wp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	The Shop Page WP WordPress plugin before 1.2.8 does not sanitise and escape some of the Product fields, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24811**	N/A	A-SHO-SHOP-061221/387
simple_jwt_login_project					
simple_jwt_login					
Cross-Site Request Forgery (CSRF)	17-Nov-21	6.8	The Simple JWT Login WordPress plugin before 3.2.1 does not have nonce checks when saving its settings, allowing attackers to make a logged in admin changed them. Settings such as HMAC verification secret, account registering and default user roles can be updated, which could result in site takeover. **CVE ID : CVE-2021-24804**	N/A	A-SIM-SIMP-061221/388
Smartertools					
smartermail					
Improper Neutralization of Input	17-Nov-21	4.3	SmarterTools SmarterMail 16.x through 100.x before 100.0.7803 allows XSS.	https://www.smartertools.com/sma	A-SMA-SMAR-061221/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2021-43977**	rtermail/release-notes/current	
N/A	17-Nov-21	7.5	SmarterTools SmarterMail 16.x through 100.x before 100.0.7803 allows remote code execution. **CVE ID : CVE-2021-32234**	https://www.smartertools.com/smartermail/release-notes/current	A-SMA-SMAR-061221/390
smashballoon					
smash_balloon_social_post_feed					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	The Smash Balloon Social Post Feed WordPress plugin before 4.0.1 did not have any privilege or nonce validation before saving the plugin's setting. As a result, any logged-in user on a vulnerable site could update the settings and store rogue JavaScript on each of its posts and pages. **CVE ID : CVE-2021-24918**	N/A	A-SMA-SMAS-061221/391
snipeitapp					
snipe-it					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Nov-21	3.5	snipe-it is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-3961**	https://huntr.dev/bounties/5987aed5-6613-4937-8a3e-d48009b7da10, https://github.com/snipe/snipe-it/commit/7	A-SNI-SNIP-061221/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ce5993f5ae9d713a0955c2fd8e2dff7a7ce886e	
Sophos					
unified_threat_management_up2date					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Nov-21	6.5	An authenticated user could potentially execute code via an SQLi vulnerability in the user portal of SG UTM before version 9.708 MR8. **CVE ID : CVE-2021-36807**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20211126-sg-sqli	A-SOP-UNIF-061221/393
Spreecommerce					
spree_auth_devise					
Cross-Site Request Forgery (CSRF)	17-Nov-21	6.8	spree_auth_devise is an open source library which provides authentication and authorization services for use with the Spree storefront framework by using an underlying Devise authentication framework. In affected versions spree_auth_devise is subject to a CSRF vulnerability that allows user account takeover. All applications using any version of the frontend component of spree_auth_devise are affected if protect_from_forgery method is both: Executed whether as: A before_action callback (the default). A prepend_before_action	https://github.com/spree/spree_auth_devise/commit/adf6ed4cd94d66091776b5febd4ff3767362de63, https://github.com/spree/spree_auth_devise/security/advisories/GHSA-26xx-m4q2-xhq8	A-SPR-SPRE-061221/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(option prepend: true given) before the :load_object hook in Spree::UserController (most likely order to find). Configured to use :null_session or :reset_session strategies (:null_session is the default in case the no strategy is given, but rails --new generated skeleton use :exception). Users are advised to update their spree_auth_devise gem. For users unable to update it may be possible to change your strategy to :exception. Please see the linked GHSA for more workaround details. ### Impact CSRF vulnerability that allows user account takeover. All applications using any version of the frontend component of `spree_auth_devise` are affected if `protect_from_forgery` method is both: * Executed whether as: * A before_action callback (the default) * A prepend_before_action (option prepend: true given) before the :load_object hook in Spree::UserController (most likely order to find). * Configured to use :null_session or :reset_session strategies (:null_session is the default in case the no strategy is given, but rails --new generated skeleton use :exception). That means that		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			applications that haven't been configured differently from what it's generated with Rails aren't affected. Thanks @waiting-for-dev for reporting and providing a patch ? ### Patches Spree 4.3 users should update to spree_auth_devise 4.4.1 Spree 4.2 users should update to spree_auth_devise 4.2.1 ### Workarounds If possible, change your strategy to :exception: ```ruby class ApplicationController < ActionController::Base protect_from_forgery with: :exception end ``` Add the following to`config/application.rb `to at least run the `:exception` strategy on the affected controller: ```ruby config.after_initialize do Spree::UsersController.protect_from_forgery with: :exception end ``` ### References https://github.com/solidusio/solidus_auth_devise/security/advisories/GHSA-xm34-v85h-9pg2 **CVE ID : CVE-2021-41275**		
ssrf-agent_project					
ssrf-agent					
Server-Side Request Forgery (SSRF)	22-Nov-21	5	The package ssrf-agent before 1.0.5 are vulnerable to Server-side Request Forgery (SSRF) via the defaultIpChecker function. It fails to properly	https://snyk.io/vuln/SNYK-JS-SSRFAGENT-1584362,	A-SSR-SSRF-061221/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate if the IP requested is private. **CVE ID : CVE-2021-23718**	https://github.com/welefen/ssrf-agent/blob/cec2b85fe8886ad6926a247a3e059d8369ec022b/index.js%23L13	
stylishcostcalculator					
stylish_cost_calculator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	The Stylish Cost Calculator WordPress plugin before 7.0.4 does not have any authorisation and CSRF checks on some of its AJAX actions (available to authenticated users), which could allow any authenticated users, such as subscriber to call them, and perform Stored Cross-Site Scripting attacks against logged in admin, as well as frontend users due to the lack of sanitisation and escaping in some parameters **CVE ID : CVE-2021-24822**	N/A	A-STY-STYL-061221/396
tammersoft					
shared_files					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	3.5	The Shared Files WordPress plugin before 1.6.61 does not sanitise and escape the Download Counter Text settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is	N/A	A-TAM-SHAR-061221/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disallowed **CVE ID : CVE-2021-24856**		
teampasswordmanager					
team_password_manager					
Cross-Site Request Forgery (CSRF)	19-Nov-21	6.8	Team Password Manager (aka TeamPasswordManager) before 10.135.236 has a CSRF vulnerability during import. **CVE ID : CVE-2021-44036**	https://teampasswordmanager.com/docs/changelog/#10.135.236	A-TEA-TEAM-061221/398
Weak Password Recovery Mechanism for Forgotten Password	19-Nov-21	5	Team Password Manager (aka TeamPasswordManager) before 10.135.236 allows password-reset poisoning. **CVE ID : CVE-2021-44037**	https://teampasswordmanager.com/docs/changelog/#10.135.236	A-TEA-TEAM-061221/399
themeum					
tutor_lms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	4.3	The Tutor LMS WordPress plugin before 1.9.11 does not sanitise and escape user input before outputting back in attributes in the Student Registration page, leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24873**	https://plugins.trac.wordpress.org/changeset/2615802/tutor	A-THE-TUTO-061221/400
Tibco					
partnerexpress					
N/A	16-Nov-21	9.3	The Interior Server and Gateway Server components of TIBCO Software Inc.'s TIBCO PartnerExpress contain an easily exploitable vulnerability that allows an unauthenticated attacker with network access to obtain	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/ad	A-TIB-PART-061221/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session tokens for the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO PartnerExpress: versions 6.2.1 and below. **CVE ID : CVE-2021-43046**	visories/2021/11/tibco-security-advisory-november-16-2021-tibco-partnerexpress-2021-43046	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-21	8.5	The Interior Server and Gateway Server components of TIBCO Software Inc.'s TIBCO PartnerExpress contain easily exploitable Stored and Reflected Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker to social engineer a legitimate user with network access to execute scripts targeting the affected system or the victim's local system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO PartnerExpress: versions 6.2.1 and below. **CVE ID : CVE-2021-43047**	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2021/11/tibco-security-advisory-november-16-2021-tibco-partnerexpress-2021-43047	A-TIB-PART-061221/402
Improper Restriction of Rendered UI Layers or Frames	16-Nov-21	10	The Interior Server and Gateway Server components of TIBCO Software Inc.'s TIBCO PartnerExpress contain a vulnerability that theoretically allows an unauthenticated attacker with network access to execute a	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/ad	A-TIB-PART-061221/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			clickjacking attack on the affected system. A successful attack using this vulnerability does not require human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO PartnerExpress: versions 6.2.1 and below. **CVE ID : CVE-2021-43048**	visories/2021/11/tibco-security-advisory-november-16-2021-tibco-partnerexpress-2021-43048	
Tightvnc					
tightvnc					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Nov-21	7.5	Buffer Overflow vulnerability in tvnviewer.exe of TightVNC Viewer allows a remote attacker to execute arbitrary instructions via a crafted FramebufferUpdate packet from a VNC server. **CVE ID : CVE-2021-42785**	https://www.tightvnc.com/whatsnew.php	A-TIG-TIGH-061221/404
Trane					
symbio_700					
Improper Control of Generation of Code ('Code Injection')	22-Nov-21	4.6	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software. **CVE ID : CVE-2021-38448**	https://us-cert.cisa.gov/ics/advisories/icsa-21-266-01	A-TRA-SYMB-061221/405
symbio_800					
Improper Control of Generation of Code ('Code	22-Nov-21	4.6	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the	https://us-cert.cisa.gov/ics/advisories/icsa-21-266-01	A-TRA-SYMB-061221/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			intended controller flow of the software. **CVE ID : CVE-2021-38448**		
transloadit					
tusdotnet					
Use of a Broken or Risky Cryptographic Algorithm	22-Nov-21	4.3	The client in tusdotnet through 2.5.0 relies on SHA-1 to prevent spoofing of file content. **CVE ID : CVE-2021-44150**	N/A	A-TRA-TUSD-061221/407
Trendmicro					
antivirus					
Incorrect Authorization	30-Nov-21	4.6	Trend Micro Antivirus for Mac 2021 v11 (Consumer) is vulnerable to an improper access control privilege escalation vulnerability that could allow an attacker to establish a connection that could lead to full local privilege escalation within the application. Please note that an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-43771**	https://helpcenter.trendmicro.com/en-us/article/TMKA-10832	A-TRE-ANTI-061221/408
Tribulant					
slideshow_gallery					
Improper Neutralization of Input During Web Page Generation ('Cross-site	23-Nov-21	3.5	The Slideshow Gallery WordPress plugin before 1.7.4 does not sanitise and escape the Slide "Title", "Description", and Gallery "Title" fields, which could allow high privilege users to	N/A	A-TRI-SLID-061221/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed **CVE ID : CVE-2021-24882**		
twmap_project					
twmap					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	4.3	An unspecified version of twmap is affected by a Cross Site Scripting (XSS) vulnerability. In file list.php, the exit function will terminate the script and print the message to the user. The message will contain $_REQUEST then there is a XSS vulnerability. **CVE ID : CVE-2021-43696**	N/A	A-TWM-TWMA-061221/410
ui					
unifi_protect					
Exposure of Resource to Wrong Sphere	24-Nov-21	6.8	A Cross-Origin Resource Sharing (CORS) vulnerability found in UniFi Protect application Version 1.19.2 and earlier allows a malicious actor who has convinced a privileged user to access a URL with malicious code to take over said user's account.This vulnerability is fixed in UniFi Protect application Version 1.20.0 and later. **CVE ID : CVE-2021-22957**	https://community.ui.com/releases/Security-Advisory-Bulletin-021-021/62bd8841-6603-4fee-9dba-73037148f173	A-UI-UNIF-061221/411
Vercot					
serva					
Buffer Copy without	29-Nov-21	5	Serva 4.4.0 allows remote attackers to cause a denial of	N/A	A-VER-SERV-061221/412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			service (daemon crash) via a TFTP read (RRQ) request, aka opcode 1, a related issue to CVE-2013-0145. **CVE ID : CVE-2021-44429**		
Vestacp					
vesta_control_panel					
N/A	29-Nov-21	7.5	vesta 0.9.8-24 is affected by a file inclusion vulnerability in file web/add/user/index.php. **CVE ID : CVE-2021-43693**	N/A	A-VES-VEST-061221/413
VIM					
vim					
Out-of-bounds Write	19-Nov-21	8.5	vim is vulnerable to Heap-based Buffer Overflow **CVE ID : CVE-2021-3968**	https://huntr.dev/bounties/00d62924-a7b4-4a61-ba29-acab2eaa1528, https://github.com/vim/vim/commit/a062006b9de0b2947ab5fb376c6e67ef92a8cd69	A-VIM-VIM-061221/414
Out-of-bounds Write	19-Nov-21	9.3	vim is vulnerable to Heap-based Buffer Overflow **CVE ID : CVE-2021-3973**	https://github.com/vim/vim/commit/615ddd5342b50a6878a907062aa471740bd9a847, https://huntr.dev/bounti	A-VIM-VIM-061221/415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				es/ce6e8609-77c6-4e17-b9fc-a2e5abed052e	
Use After Free	19-Nov-21	6.8	vim is vulnerable to Use After Free **CVE ID : CVE-2021-3974**	https://github.com/vim/vim/commit/64066b9acd9f8cffdf4840f797748f938a13f2d6, https://huntr.dev/bounties/e402cb2c-8ec4-4828-a692-c95f8e0de6d4	A-VIM-VIM-061221/416
Vmware					
cloud_foundation					
Exposure of Sensitive Information to an Unauthorized Actor	24-Nov-21	5	The vSphere Web Client (FLEX/Flash) contains an unauthorized arbitrary file read vulnerability. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information. **CVE ID : CVE-2021-21980**	https://www.vmware.com/security/advisories/VMSA-2021-0027.html	A-VMW-CLOU-061221/417
spring_cloud_netflix					
Improper Control of Generation of Code ('Code Injection')	19-Nov-21	6.5	Applications using both `spring-cloud-netflix-hystrix-dashboard` and `spring-boot-starter-thymeleaf` expose a way to execute code submitted within the request URI path during the	https://tanzu.vmware.com/security/cve-2021-22053	A-VMW-SPRI-061221/418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resolution of view templates. When a request is made at `/hystrix/monitor;[user-provided data]`, the path elements following `hystrix/monitor` are being evaluated as SpringEL expressions, which can lead to code execution. **CVE ID : CVE-2021-22053**		
vcenter_server					
Exposure of Sensitive Information to an Unauthorized Actor	24-Nov-21	5	The vSphere Web Client (FLEX/Flash) contains an unauthorized arbitrary file read vulnerability. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information. **CVE ID : CVE-2021-21980**	https://www.vmware.com/security/advisories/VMSA-2021-0027.html	A-VMW-VCEN-061221/419
Server-Side Request Forgery (SSRF)	24-Nov-21	7.5	The vSphere Web Client (FLEX/Flash) contains an SSRF (Server Side Request Forgery) vulnerability in the vSAN Web Client (vSAN UI) plug-in. A malicious actor with network access to port 443 on vCenter Server may exploit this issue by accessing a URL request outside of vCenter Server or accessing an internal service. **CVE ID : CVE-2021-22049**	https://www.vmware.com/security/advisories/VMSA-2021-0027.html	A-VMW-VCEN-061221/420
wazuh					
wazuh					
Improper Neutralizatio	22-Nov-21	7.5	In the wazuh-slack active response script in Wazuh	https://github.com/waz	A-WAZ-WAZU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			before 4.2.5, untrusted user agents are passed to a curl command line, potentially resulting in remote code execution. **CVE ID : CVE-2021-44079**	uh/wazuh/pull/10809	061221/421
We-con					
plc_editor					
Stack-based Buffer Overflow	22-Nov-21	6.8	PLC Editor Versions 1.3.8 and prior is vulnerable to a stack-based buffer overflow while processing project files, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2021-42705**	N/A	A-WE--PLC_-061221/422
Out-of-bounds Write	22-Nov-21	6.8	PLC Editor Versions 1.3.8 and prior is vulnerable to an out-of-bounds write while processing project files, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2021-42707**	N/A	A-WE--PLC_-061221/423
webfactoryltd					
wp_reset_pro					
Cross-Site Request Forgery (CSRF)	18-Nov-21	6.8	Cross-Site Request Forgery (CSRF) vulnerability leading to Database Reset in WordPress WP Reset PRO Premium plugin (versions <= 5.98) allows attackers to trick authenticated into making unintentional database reset. **CVE ID : CVE-2021-36908**	https://wpreset.com/changelog/, https://patchstack.com/wp-reset-pro-critical-vulnerability-fixed/	A-WEB-WP_R-061221/424
Incorrect Authorization	18-Nov-21	5.5	Authenticated Database Reset vulnerability in WordPress WP Reset PRO Premium plugin (versions <= 5.98)	https://wpreset.com/changelog/	A-WEB-WP_R-061221/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows any authenticated user to wipe the entire database regardless of their authorization. It leads to a complete website reset and takeover. **CVE ID : CVE-2021-36909**		
webventures					
client_invoicing_by_sprout_invoices					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	3.5	The Client Invoicing by Sprout Invoices WordPress plugin before 19.9.7 does not sanitise and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24787**	N/A	A-WEB-CLIE-061221/426
wipro					
holmes					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Nov-21	5	The File Download API in Wipro Holmes Orchestrator 20.4.1 (20.4.1_02_11_2020) allows remote attackers to read arbitrary files via absolute path traversal in the SearchString JSON field in /home/download POST data. **CVE ID : CVE-2021-38146**	N/A	A-WIP-HOLM-061221/427
Missing Authentication for Critical Function	29-Nov-21	5	Wipro Holmes Orchestrator 20.4.1 (20.4.1_02_11_2020) allows remote attackers to download arbitrary files, such as reports containing sensitive information, because authentication is not	N/A	A-WIP-HOLM-061221/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required for API access to processexecution/DownloadExcelFile/Domain_Credential_Report_Excel, processexecution/DownloadExcelFile/User_Report_Excel, processexecution/DownloadExcelFile/Process_Report_Excel, processexecution/DownloadExcelFile/Infrastructure_Report_Excel, or processexecution/DownloadExcelFile/Resolver_Report_Excel. **CVE ID : CVE-2021-38147**		
Insertion of Sensitive Information into Log File	29-Nov-21	5	Wipro Holmes Orchestrator 20.4.1 (20.4.1_02_11_2020) allows remote attackers to read application log files containing sensitive information via a predictable /log URI. **CVE ID : CVE-2021-38283**	N/A	A-WIP-HOLM-061221/429
Wireshark					
wireshark					
NULL Pointer Dereference	18-Nov-21	5	NULL pointer exception in the IPPUSB dissector in Wireshark 3.4.0 to 3.4.9 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2021-39920**	https://www.wireshark.org/security/wnpa-sec-2021-15.html, https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39920.json	A-WIR-WIRE-061221/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	19-Nov-21	5	NULL pointer exception in the Modbus dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2021-39921**	https://www.wireshark.org/security/wnpa-sec-2021-14.html, https://gitlab.com/wireshark/wireshark/-/issues/17703, https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39921.json	A-WIR-WIRE-061221/431
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Nov-21	5	Buffer overflow in the C12.22 dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2021-39922**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39922.json, https://www.wireshark.org/security/wnpa-sec-2021-12.html, https://gitlab.com/wireshark/wireshark/-/issues/17636	A-WIR-WIRE-061221/432
NULL Pointer	19-Nov-21	5	NULL pointer exception in the IPPUSB dissector in	https://gitlab.com/gitlab	A-WIR-WIRE-061221/433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			Wireshark 3.4.0 to 3.4.9 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2021-39923**	-org/cves/-/blob/master/2021/CVE-2021-39923.json, https://gitlab.com/wireshark/wireshark/-/issues/17705, https://www.wireshark.org/security/wnpa-sec-2021-15.html	
Excessive Iteration	19-Nov-21	5	Large loop in the Bluetooth DHT dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2021-39924**	https://www.wireshark.org/security/wnpa-sec-2021-10.html, https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39924.json, https://gitlab.com/wireshark/wireshark/-/issues/17677	A-WIR-WIRE-061221/434
Buffer Copy without Checking Size of Input	19-Nov-21	5	Buffer overflow in the Bluetooth SDP dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of	https://gitlab.com/gitlab-org/cves/-/blob/maste	A-WIR-WIRE-061221/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			service via packet injection or crafted capture file **CVE ID : CVE-2021-39925**	r/2021/CVE-2021-39925.json, https://www.wireshark.org/security/wnpa-sec-2021-09.html, https://gitlab.com/wireshark/wireshark/-/issues/17635	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Nov-21	5	Buffer overflow in the Bluetooth HCI_ISO dissector in Wireshark 3.4.0 to 3.4.9 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2021-39926**	https://gitlab.com/wireshark/wireshark/-/issues/17649, https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39926.json, https://www.wireshark.org/security/wnpa-sec-2021-08.html	A-WIR-WIRE-061221/436
NULL Pointer Dereference	18-Nov-21	5	NULL pointer exception in the IEEE 802.11 dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of service via packet injection or crafted capture file	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-	A-WIR-WIRE-061221/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39928	39928.json, https://www.wireshark.org/security/wnpa-sec-2021-13.html	
Uncontrolled Recursion	19-Nov-21	5	Uncontrolled Recursion in the Bluetooth DHT dissector in Wireshark 3.4.0 to 3.4.9 and 3.2.0 to 3.2.17 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2021-39929**	https://gitlab.com/wireshark/wireshark/-/issues/17651, https://www.wireshark.org/security/wnpa-sec-2021-07.html, https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39929.json	A-WIR-WIRE-061221/438
Wordpress					
wordpress					
N/A	25-Nov-21	7.5	WordPress before 5.8 lacks support for the Update URI plugin header. This makes it easier for remote attackers to execute arbitrary code via a supply-chain attack against WordPress installations that use any plugin for which the slug satisfies the naming constraints of the WordPress.org Plugin Directory but is not yet	https://make.wordpress.org/core/2021/06/29/introducing-update-uri-plugin-header-in-wordpress-5-8/	A-WOR-WORD-061221/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			present in that directory. **CVE ID : CVE-2021-44223**		
wordpress_popular_posts_project					
wordpress_popular_posts					
Unrestricted Upload of File with Dangerous Type	17-Nov-21	6.5	The WordPress Popular Posts WordPress plugin is vulnerable to arbitrary file uploads due to insufficient input file type validation found in the ~/src/Image.php file which makes it possible for attackers with contributor level access and above to upload malicious files that can be used to obtain remote code execution, in versions up to and including 5.3.2. **CVE ID : CVE-2021-42362**	https://plugins.trac.wordpress.org/changeset/2542638/wordpress-popular-posts/trunk/src/Image.php	A-WOR-WORD-061221/440
workerman-thinkphp-redis_project					
workerman-thinkphp-redis					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	4.3	An unspecified version of Workerman-ThinkPHP-Redis is affected by a Cross Site Scripting (XSS) vulnerability. In file Controller.class.php, the exit function will terminate the script and print the message to the user. The message will contain $_GET{C('VAR_JSONP_HANDLER')] then there is a XSS vulnerability. **CVE ID : CVE-2021-43697**	N/A	A-WOR-WORK-061221/441
wp-buy					
seo_redirection-301_redirect_manager					
Improper Neutralizatio	17-Nov-21	6.5	The importFromRedirection AJAX action of the SEO	N/A	A-WP--SEO_-061221/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an SQL Command ('SQL Injection')			Redirection Plugin â€“ 301 Redirect Manager WordPress plugin before 8.2, available to any authenticated user, does not properly sanitise the offset parameter before using it in a SQL statement, leading an SQL injection when the redirection plugin is also installed **CVE ID : CVE-2021-24847**		
wpchill					
check_\\&_log_email					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	2.6	The Check & Log Email WordPress plugin before 1.0.4 does not escape the d parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2021-24908**	N/A	A-WPC-CHEC-061221/443
wpdeveloper					
betterlinks					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	3.5	The BetterLinks WordPress plugin before 1.2.6 does not sanitise and escape some of imported link fields, which could lead to Stored Cross-Site Scripting issues when an admin import a malicious CSV. **CVE ID : CVE-2021-24812**	N/A	A-WPD-BETT-061221/444
wpkube					
about_author_box					
Improper Neutralization of Input	29-Nov-21	3.5	The About Author Box WordPress plugin before 1.0.2 does not sanitise and escape	N/A	A-WPK-ABOU-061221/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			the Social Profiles field values before outputting them in attributes, which could allow user with a role as low as contributor to perform Cross-Site Scripting attacks. **CVE ID : CVE-2021-24745**		
wpo365					
wordpress_\\+_azure_ad_\\/_microsoft_office_365					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Nov-21	4.3	The "WPO365 | LOGIN" WordPress plugin (up to and including version 15.3) by wpo365.com is vulnerable to a persistent Cross-Site Scripting (XSS) vulnerability (also known as Stored or Second-Order XSS). Persistent XSS vulnerabilities occur when the application stores and retrieves client supplied data without proper handling of dangerous content. This type of XSS vulnerability is exploited by submitting malicious script content to the application which is then retrieved and executed by other application users. The attacker could exploit this to conduct a range of attacks against users of the affected application such as session hijacking, account take over and accessing sensitive data. In this case, the XSS payload can be submitted by any anonymous user, the payload then renders and executes when a WordPress administrator authenticates	https://www.wpo365.com/change-log/	A-WPO-WORD-061221/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and accesses the WordPress Dashboard. The injected payload can carry out actions on behalf of the administrator including adding other administrative users and changing application settings. This flaw could be exploited to ultimately provide full control of the affected system to the attacker. **CVE ID : CVE-2021-43409**		
wpplugin					
accept_donations_with_paypal					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	3.5	The Accept Donations with PayPal WordPress plugin before 1.3.2 does not escape the Amount Menu Name field of created Buttons, which could allow a high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24815**	N/A	A-WPP-ACCE-061221/447
wprssaggregator					
wp_rss_aggregator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	The WP RSS Aggregator WordPress plugin before 4.19.2 does not properly sanitise and escape the URL to Blacklist field, allowing malicious HTML to be inserted by high privilege users even when the unfiltered_html capability is disallowed, which could lead to Cross-Site Scripting issues.	N/A	A-WPR-WP_R-061221/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24768		
wpshopmart					
testimonial_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	3.5	The Testimonial WordPress plugin before 1.6.0 does not escape some testimonial fields which could allow high privilege users to perform Cross Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24598**	https://plugins.trac.wordpress.org/changeset/2606523/	A-WPS-TEST-061221/449
wpwave					
hide_my_wp					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Nov-21	7.5	The SQL injection vulnerability in the Hide My WP WordPress plugin (versions <= 6.2.3) is possible because of how the IP address is retrieved and used inside a SQL query. The function "hmwp_get_user_ip" tries to retrieve the IP address from multiple headers, including IP address headers that the user can spoof, such as "X-Forwarded-For." As a result, the malicious payload supplied in one of these IP address headers will be directly inserted into the SQL query, making SQL injection possible. **CVE ID : CVE-2021-36916**	https://codecanyon.net/item/hide-my-wp-amazing-security-plugin-for-wordpress/4177158, https://patchstack.com/database/vulnerability/hide-my-wp/wordpress-hide-my-wp-premium-plugin-6-2-3-sql-injection-sqli-vulnerability	A-WPW-HIDE-061221/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	24-Nov-21	5	WordPress Hide My WP plugin (versions <= 6.2.3) can be deactivated by any unauthenticated user. It is possible to retrieve a reset token which can then be used to deactivate the plugin. **CVE ID : CVE-2021-36917**	https://codecanyon.net/item/hide-my-wp-amazing-security-plugin-for-wordpress/4177158	A-WPW-HIDE-061221/451
wp_performance_score_booster_project					
wp_performance_score_booster					
Cross-Site Request Forgery (CSRF)	17-Nov-21	4.3	The WP Performance Score Booster WordPress plugin before 2.1 does not have CSRF check when saving its settings, which could allow attackers to make a logged in admin change them via a CSRF attack. **CVE ID : CVE-2021-24776**	N/A	A-WP_-WP_P-061221/452
xml-sitemaps					
unlimited_sitemap_generator					
Cross-Site Request Forgery (CSRF)	24-Nov-21	6.8	Cross-site request forgery (CSRF) vulnerability in Unlimited Sitemap Generator versions prior to v8.2 allows a remote attacker to hijack the authentication of an administrator and conduct arbitrary operation via a specially crafted web page. **CVE ID : CVE-2021-20845**	https://www.xml-sitemaps.com/news-20210831.html, https://www.xml-sitemaps.com/standalone-google-sitemap-generator.html	A-XML-UNLI-061221/453
xwp					
stream					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Nov-21	6.5	The Stream WordPress plugin before 3.8.2 does not sanitise and validate the order GET parameter from the Stream Records admin dashboard before using it in a SQL statement, leading to an SQL injection issue. **CVE ID : CVE-2021-24772**	https://plugins.trac.wordpress.org/changeset/2615811/stream	A-XWP-STRE-061221/454
yop-poll					
yop_poll					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	3.5	The YOP Poll WordPress plugin before 6.3.1 is affected by a stored Cross-Site Scripting vulnerability, which exists in the Admin preview module where a user with a role as low as author is allowed to execute arbitrary script code within the context of the application. This vulnerability is due to insufficient validation of question and answer text parameters in Create Poll module. **CVE ID : CVE-2021-24833**	https://plugins.trac.wordpress.org/changeset/2605368	A-YOP-YOP_-061221/455
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-21	4.3	The YOP Poll WordPress plugin before 6.3.1 is affected by a stored Cross-Site Scripting vulnerability which exists in the Create Poll - Options module where a user with a role as low as author is allowed to execute arbitrary script code within the context of the application. This vulnerability is due to insufficient validation of	https://plugins.trac.wordpress.org/changeset/2605368	A-YOP-YOP_-061221/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			custom label parameters - vote button label , results link label and back to vote caption label. **CVE ID : CVE-2021-24834**		
youtubephpmirroring_project					
youtube-php-mirroring					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	4.3	An unspecified version of youtube-php-mirroring is affected by a Cross Site Scripting (XSS) vulnerability in file ytproxy/index.php. **CVE ID : CVE-2021-43692**	N/A	A-YOU-YOUT-061221/457
Zoho					
manageengine_remote_access_plus_server					
Improper Privilege Management	17-Nov-21	6.5	Zoho Remote Access Plus Server Windows Desktop Binary fixed in 10.1.2132.6 is affected by a sensitive information disclosure vulnerability. Due to improper privilege management, the process launches as the logged in user, so memory dump can be done by non-admin also. Remotely, an attacker can dump all sensitive information including DB Connection string, entire IT infrastructure details, commands executed by IT admin including credentials, secrets, private keys and more. **CVE ID : CVE-2021-42956**	N/A	A-ZOH-MANA-061221/458
Zohocorp					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
manageengine_remote_access_plus					
Incorrect Authorization	17-Nov-21	4.6	Zoho Remote Access Plus Server Windows Desktop Binary fixed from 10.1.2121.1 is affected by incorrect access control. The installation directory is vulnerable to weak file permissions by allowing full control for Windows Everyone user group (non-admin or any guest users), thereby allowing privilege escalation, unauthorized password reset, stealing of sensitive data, access to credentials in plaintext, access to registry values, tampering with configuration files, etc. **CVE ID : CVE-2021-42954**	N/A	A-ZOH-MANA-061221/459
Incorrect Authorization	17-Nov-21	7.2	Zoho Remote Access Plus Server Windows Desktop binary fixed in version 10.1.2132 is affected by an unauthorized password reset vulnerability. Because of the designed password reset mechanism, any non-admin Windows user can reset the password of the Remote Access Plus Server Admin account. **CVE ID : CVE-2021-42955**	N/A	A-ZOH-MANA-061221/460
zrlog					
zrlog					
Unrestricted Upload of File with Dangerous	28-Nov-21	7.5	A Remote Command Execution vulnerability on the background in zrlog 2.2.2, at the upload avatar function,	N/A	A-ZRL-ZRLO-061221/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type			could bypass the original limit, upload the JSP file to get a WebShell **CVE ID : CVE-2021-44093**		
Unrestricted Upload of File with Dangerous Type	28-Nov-21	6.8	ZrLog 2.2.2 has a remote command execution vulnerability at plugin download function, it could execute any JAR file **CVE ID : CVE-2021-44094**	N/A	A-ZRL-ZRLO-061221/462
Hardware					
ABB					
rtu500					
Improper Input Validation	26-Nov-21	7.1	Improper Input Validation vulnerability in the APDU parser in the Bidirectional Communication Interface (BCI) IEC 60870-5-104 function of Hitachi Energy RTU500 series allows an attacker to cause the receiving RTU500 CMU of which the BCI is enabled to reboot when receiving a specially crafted message. By default, BCI IEC 60870-5-104 function is disabled (not configured). This issue affects: Hitachi Energy RTU500 series CMU Firmware version 12.0.* (all versions); CMU Firmware version 12.2.* (all versions); CMU Firmware version 12.4.* (all versions). **CVE ID : CVE-2021-35533**	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000063&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-RTU5-061221/463
AMD					
epyc_7001					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/464
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/465
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/466
epyc_7002					
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/467
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2021-26331**	sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/469
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/470
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/471
epyc_7003					
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**		
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/473
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/474
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/475
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/476
Improper Restriction	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit	https://www.amd.com/	H-AMD-EPYC-061221/477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			(SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	en/corporate/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/478
epyc_7232p					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/479
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/480
Improper	16-Nov-21	4.9	Insufficient ID command	https://ww	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	061221/481
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/482
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/483
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/484
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/485
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	security/bulletin/amd-sb-1021	
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/487
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/488
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/489
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/490
N/A	16-Nov-21	2.1	Insufficient DRAM address	https://ww	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	061221/491
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/492
epyc_7251					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/493
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/495
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/496
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/497
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/498
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/499
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform	https://www.amd.com/	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	en/corporate/product-security/bulletin/amd-sb-1021	061221/500
epyc_7252					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/501
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/502
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/504
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/505
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/506
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/507
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/508

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/509
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/510
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/511
epyc_7261					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/512

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26312		
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/513
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/514
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/515
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/516
epyc_7262					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/518
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/519
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/520
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/521
Out-of-	16-Nov-21	2.1	AMD System Management	https://ww	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	061221/522
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/523
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/524
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/525
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			servicing further requests. **CVE ID : CVE-2021-26337**	sb-1021	
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/527
epyc_7272					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/528
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/529
Improper Neutralization of Special Elements used in a	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			the PSP. **CVE ID : CVE-2021-26321**	etin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/531
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/532
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/533
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/534
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/536
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/537
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/538
epyc_7281					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/540
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/541
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/542
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/543
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may result in a loss of resources. **CVE ID : CVE-2021-26330**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/545
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/546
epyc_7282					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/547
Improper Certificate	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK)	https://www.amd.com/	H-AMD-EPYC-061221/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	en/corporate/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/549
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/550
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/551
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/552
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/554
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/555
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/556
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26338**		
epyc_72f3					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/558
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/559
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/560
Improper Neutralizatio	16-Nov-21	4.9	Insufficient ID command validation in the SEV	https://www.amd.com/	H-AMD-EPYC-061221/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	en/corporate/product-security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/562
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/563
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/564
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/565
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				etin/amd-sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/567
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/568
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/569
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/570
Improper Restriction of Operations	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/572
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/573
epyc_7301					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/574
Improper Certificate	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK)	https://www.amd.com/	H-AMD-EPYC-061221/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	en/corporate/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/576
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/577
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/578
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/579
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/581
epyc_7302					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/582
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/583
Improper Neutralizatio	16-Nov-21	4.9	Insufficient ID command validation in the SEV	https://www.amd.com/	H-AMD-EPYC-061221/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	en/corporate/product-security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/585
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/586
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/587
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/588
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	security/bulletin/amd-sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/590
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/591
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/592
epyc_7302p					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects:	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	etin/amd-sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/594
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/595
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/596
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/598
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/599
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/600
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/601
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	etin/amd-sb-1021	
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/603
epyc_7313					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/604
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/606
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/607
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/608
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/609
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/610
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during	https://www.amd.com/	H-AMD-EPYC-061221/611

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	en/corporate/product-security/bulletin/amd-sb-1021	
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/612
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/613
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/614
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/615
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	etin/amd-sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/617
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/618
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/619
epyc_7313p					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	sb-1021	
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/621
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/622
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/623
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/624

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack”. **CVE ID : CVE-2021-26322**	security/bulletin/amd-sb-1021	
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/625
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/626
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/627
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/628
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/630
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/631
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/632
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/633
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	etin/amd-sb-1021	
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/635
epyc_7343					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/636
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/638
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/639
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/640
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/641
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/642
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during	https://www.amd.com/	H-AMD-EPYC-061221/643

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	en/corporate/product-security/bulletin/amd-sb-1021	
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/644
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/645
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/646
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/647
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	etin/amd-sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/649
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/650
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/651
epyc_7351					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/653
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/654
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/655
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/656
Out-of-	16-Nov-21	2.1	AMD System Management	https://ww	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	061221/657
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/658
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/659
epyc_7351p					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/661
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/662
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/663
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/664
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/665
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a	https://www.amd.com/	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	en/corporate/product-security/bulletin/amd-sb-1021	061221/666
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/667
epyc_7352					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/668
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/670
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/671
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/672
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/673
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/674
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform	https://www.amd.com/	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	en/corporate/product-security/bulletin/amd-sb-1021	061221/675
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/676
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/677
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/678
epyc_7371					
Exposure of Resource to Wrong	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	e/product-security/bulletin/amd-sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/680
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/681
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/682
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources.	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26329	sb-1021	
epyc_73f3					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/684
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/685
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/686
Improper Neutralization of Special	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	e/product-security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/688
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/689
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/690
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/691
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/693
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/694
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/695
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/696
Improper Restriction of Operations within the	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	etin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/698
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/699
epyc_7401					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/700
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	e/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/702
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/703
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/704
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/705
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	etin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/707
epyc_7401p					
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/708
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/709
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26335		
epyc_7402					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/711
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/712
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/713
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/715
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/716
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/717
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/718
Improper Restriction of Operations within the Bounds of a Memory	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/719

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			from other components. **CVE ID : CVE-2021-26336**		
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/720
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/721
epyc_7402p					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/722
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	etin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/724
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/725
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/726
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/727
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2021-26331**	sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/729
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/730
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/731
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
epyc_7413					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/733
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/734
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/735
Improper Neutralization of Special Elements used in a	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			the PSP. **CVE ID : CVE-2021-26321**	etin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/737
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/738
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/739
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/740
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/741
Integer	16-Nov-21	2.1	AMD System Management	https://ww	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	061221/742
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/743
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/744
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/745
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/746

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26336		
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/747
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/748
epyc_7443					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/749
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/751
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/752
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/753
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/754
Improper Input	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	e/product-security/bulletin/amd-sb-1021	
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/756
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/757
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/758
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/759
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26331		
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/761
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/762
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/763
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/764
epyc_7443p					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/765
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/766
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/767
Improper Neutralization of Special Elements used in a Command	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP.	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			**CVE ID : CVE-2021-26321**	sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/769
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/770
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/771
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/772
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/773
Integer Overflow or	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience	https://www.amd.com/	H-AMD-EPYC-061221/774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	en/corporate/product-security/bulletin/amd-sb-1021	
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/775
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/776
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/777
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26336		
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/779
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/780
epyc_7451					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/781
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of service of the PSP **CVE ID : CVE-2021-26320**	sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/783
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/784
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/785
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/786
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26331		
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/788
epyc_7452					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/789
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/790
Improper Neutralization of Special Elements used in a	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			the PSP. **CVE ID : CVE-2021-26321**	etin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/792
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/793
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/794
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/795
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/797
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/798
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/799
epyc_7453					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/801
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/802
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/803
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”.	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26322	sb-1021	
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/805
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/806
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/807
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/808
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/809
Out-of-bounds	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			may result in a loss of resources. **CVE ID : CVE-2021-26330**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/811
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/812
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/813
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26337		
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/815
epyc_74f3					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/816
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/817
Improper Certificate	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK)	https://www.amd.com/	H-AMD-EPYC-061221/818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	en/corporate/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/819
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/820
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/821
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/822
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity.	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26326	security/bulletin/amd-sb-1021	
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/824
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/825
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/826
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/827
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/829
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/830
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/831
epyc_7501					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/833
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/834
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/835
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/836
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may result in a loss of resources. **CVE ID : CVE-2021-26330**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/838
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/839
epyc_7502					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/840
Improper Certificate	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK)	https://www.amd.com/	H-AMD-EPYC-061221/841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	en/corporate/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/842
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/843
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/844
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/845
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/847
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/848
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/849
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26338**		
epyc_7502p					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/851
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/852
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/853
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/855
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/856
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/857
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/858
Improper Restriction of Operations within the	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	etin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/860
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/861
epyc_7513					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/862
Insufficient Verification of Data	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authenticity			subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	e/product-security/bulletin/amd-sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/864
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/865
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/866
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/868
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/869
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/870
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/871
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/872
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/874
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/875
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/876
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26338**		
epyc_7532					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/878
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/879
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/880
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/882
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/883
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/884
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/885
Improper Restriction of Operations within the	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	etin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/887
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/888
epyc_7542					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/889
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	e/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/891
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/892
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/893
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/894
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	etin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/896
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/897
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/898
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26338		
epyc_7543					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/900
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/901
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/902
Improper Neutralization of Special	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	e/product-security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/904
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/905
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/906
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/907
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/909
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/910
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/911
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/912
Improper Restriction of Operations within the	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	etin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/914
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/915
epyc_7543p					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/916
Insufficient Verification of Data	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authenticity			subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	e/product-security/bulletin/amd-sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/918
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/919
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/920
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/922
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/923
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/924
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/925
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/926
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/928
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/929
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/930
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26338**		
epyc_7551					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/932
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/933
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/934
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/936
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/937
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/938
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/939
epyc_7551p					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	security/bulletin/amd-sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/941
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/942
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/943
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/944

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/945
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/946
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/947
epyc_7552					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/948

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/949
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/950
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/951
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/952
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/953
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a	https://www.amd.com/	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	en/corporate/product-security/bulletin/amd-sb-1021	061221/954
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/955
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/956
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/957
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/958

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potential lack of system resources. **CVE ID : CVE-2021-26338**	sb-1021	
epyc_75f3					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/959
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/960
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/961
Improper	16-Nov-21	4.9	Insufficient ID command	https://ww	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	061221/962
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/963
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/964
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/965
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/966
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality.	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26327	security/bulletin/amd-sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/968
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/969
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/970
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/971
Improper Restriction of	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/973
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/974
epyc_7601					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/975
Improper	16-Nov-21	2.1	Insufficient validation of the	https://ww	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Certificate Validation			AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	061221/976
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/977
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/978
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/979
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/980
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/982
epyc_7642					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/983
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/984
Improper	16-Nov-21	4.9	Insufficient ID command	https://ww	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	061221/985
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/986
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/987
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/988
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/989
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	e/product-security/bulletin/amd-sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/991
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/992
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/993
epyc_7643					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	security/bulletin/amd-sb-1021	
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/995
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/996
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/997
Use of Insufficiently	16-Nov-21	5	Persistent platform private key may not be protected	https://www.amd.com/	H-AMD-EPYC-061221/998

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Random Values			with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	en/corporate/product-security/bulletin/amd-sb-1021	
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/999
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1000
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1001
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1002
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources.	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26329	sb-1021	
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1004
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1005
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1006
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1007
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1009
epyc_7662					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1010
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1011
Improper Neutralizatio	16-Nov-21	4.9	Insufficient ID command validation in the SEV	https://www.amd.com/	H-AMD-EPYC-061221/1012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	en/corporate/product-security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1013
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1014
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1015
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1016
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/1017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	security/bulletin/amd-sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1018
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1019
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1020
epyc_7663					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects:	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/1021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	etin/amd-sb-1021	
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1022
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1023
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1024
Use of Insufficiently Random	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Values			potential "two time pad attack". **CVE ID : CVE-2021-26322**	e/product-security/bulletin/amd-sb-1021	
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1026
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1027
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1028
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1029
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1031
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1032
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1033
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1034
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to	https://www.amd.com/en/corporate/product-security/bull	H-AMD-EPYC-061221/1035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	etin/amd-sb-1021	
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1036
epyc_7702					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1037
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1038
Improper Neutralization of Special Elements	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/1039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1040
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1041
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1042
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1043
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/1044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1045
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1046
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1047
epyc_7702p					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1049
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1050
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1051
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1052
Out-of-bounds	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a	https://www.amd.com/	H-AMD-EPYC-061221/1053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	en/corporate/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1054
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1055
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1056
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1057

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26337		
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1058
epyc_7713					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1059
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1060
Improper Certificate	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK)	https://www.amd.com/	H-AMD-EPYC-061221/1061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	en/corporate/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1062
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1063
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1064
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1065
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity.	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/1066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26326	security/bulletin/amd-sb-1021	
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1067
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1068
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1069
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1070
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/1071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1072
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1073
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1074
epyc_7713p					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1076
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1077
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1078
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”.	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/1079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26322	sb-1021	
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1080
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1081
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1082
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1083
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1084
Out-of-bounds	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			may result in a loss of resources. **CVE ID : CVE-2021-26330**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1086
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1087
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1088
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26337		
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1090
epyc_7742					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1091
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1092
Improper Neutralization of Special Elements used in a Command	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP.	https://www.amd.com/en/corporate/product-security/bulletin/amd-	H-AMD-EPYC-061221/1093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			**CVE ID : CVE-2021-26321**	sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1094
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1095
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1096
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1097
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2021-26335**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1099
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1100
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1101
epyc_7763					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1103
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1104
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1105
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1106

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1107
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1108
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1109
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1110
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1111
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26330**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1113
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1114
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1115
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1117
epyc_7f32					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1118
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1119
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1120

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1121
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1122
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1123
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1124
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1125

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1126
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1127
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1128
epyc_7f52					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1129

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26312		
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1130
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1131
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1132
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1133
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1135
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1136
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1137
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1138
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-061221/1139

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	security/bulletin/amd-sb-1021	
epyc_7f72					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1140
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1141
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1142
Use of Insufficiently Random	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a	https://www.amd.com/en/corporat	H-AMD-EPYC-061221/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Values			potential "two time pad attack". **CVE ID : CVE-2021-26322**	e/product-security/bulletin/amd-sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1144
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1145
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1146
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1147
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System	https://www.amd.com/	H-AMD-EPYC-061221/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	en/corporate/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1149
epyc_7h12					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1150
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1151
Improper	16-Nov-21	4.9	Insufficient ID command	https://ww	H-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	061221/1152
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1153
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1154
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	H-AMD-EPYC-061221/1155
Asus					
gt-ax11000					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-	https://www.asus.com/Networking-IoT-Servers/WiFi-	H-ASU-GT-A-061221/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS	H-ASU-GT-A-061221/1157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/, http://asus.com	
rt-ax3000					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-RT-A-061221/1158
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/,	H-ASU-RT-A-061221/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
rt-ax55					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-RT-A-061221/1160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-RT-A-061221/1161
rt-ax56u					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-	H-ASU-RT-A-061221/1162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-RT-A-061221/1163
rt-ax56u_v2					
Improper Restriction of Excessive	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG	https://www.asus.com/Networking-	H-ASU-RT-A-061221/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-	H-ASU-RT-A-061221/1165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
rt-ax58u					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-RT-A-061221/1166
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S),	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-	H-ASU-RT-A-061221/1167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
rt-ax68u					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request.	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS	H-ASU-RT-A-061221/1168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-41435	/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-RT-A-061221/1169
rt-ax82u					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/,	H-ASU-RT-A-061221/1170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-RT-A-061221/1171
rt-ax82u_gundam_edition					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-RT-A-061221/1172
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiF	H-ASU-RT-A-061221/1173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	i-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
rt-ax86s					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-RT-A-061221/1174
Inconsistent Interpretation of HTTP Requests ('HTTP	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-	https://www.asus.com/Networking-IoT-Servers/WiF	H-ASU-RT-A-061221/1175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Smuggling')			AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	i-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
rt-ax86u					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-	H-ASU-RT-A-061221/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-RT-A-061221/1177
rt-ax86u_zaku_ii_edition					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-	H-ASU-RT-A-061221/1178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.c	H-ASU-RT-A-061221/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om	
rt-ax88u					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-RT-A-061221/1180
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/	H-ASU-RT-A-061221/1181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
rt-ax92u					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-RT-A-061221/1182
Inconsistent Interpretatio	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS	https://www.asus.com/	H-ASU-RT-A-061221/1183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of HTTP Requests ('HTTP Request Smuggling')			ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
tuf-ax5400					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiF	H-ASU-TUF--061221/1184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	i-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-TUF--061221/1185
tuf_gaming_ax3000					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U,	https://www.asus.com/Networking-IoT-Servers/WiF	H-ASU-TUF_-061221/1186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	i-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet.	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/Hel	H-ASU-TUF_-061221/1187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-41436	pDesk_BIOS/, http://asus.com	
zenwifi_ax_\\(xt8\\)					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-ZENW-061221/1188
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/Help	H-ASU-ZENW-061221/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	Desk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
zenwifi_xd6					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.c	H-ASU-ZENW-061221/1190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	H-ASU-ZENW-061221/1191
Dell					
x1008					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-	H-DEL-X100-061221/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				multiple-security-vulnerabilities	
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X100-061221/1193
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X100-061221/1194
x1008p					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an	https://www.dell.com/support/kbd	H-DEL-X100-061221/1195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	oc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X100-061221/1196
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections.	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-	H-DEL-X100-061221/1197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36322	update-for-multiple-security-vulnerabilities	
x1018					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X101-061221/1198
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X101-061221/1199
Improper Neutralizatio	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to	https://www.dell.com/s	H-DEL-X101-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements in Output Used by a Downstream Component ('Injection')			3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	upport/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	061221/1200
x1018p					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X101-061221/1201
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service.	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-	H-DEL-X101-061221/1202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36321	x-series-security-update-for-multiple-security-vulnerabilities	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X101-061221/1203
x1026					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X102-061221/1204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X102-061221/1205
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X102-061221/1206
x1026p					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-	H-DEL-X102-061221/1207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X102-061221/1208
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabiliti	H-DEL-X102-061221/1209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				es	
x1052					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X105-061221/1210
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X105-061221/1211
Improper Neutralization of Special Elements in Output Used by a	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-	H-DEL-X105-061221/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Downstream Component ('Injection')			exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	
x1052p					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X105-061221/1213
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-	H-DEL-X105-061221/1214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				security-vulnerabilities	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X105-061221/1215
x4012					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X401-061221/1216
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability.	https://www.dell.com/support/kbdoc/en-	H-DEL-X401-061221/1217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	H-DEL-X401-061221/1218
Dlink					
dwr-932c					
Missing Authentication for Critical Function	23-Nov-21	10	Missing Authentication for Critical Function vulnerability in debug_post_set.cgi of D-Link DWR-932C E1 firmware allows an unauthenticated attacker to execute administrative actions. **CVE ID : CVE-2021-42783**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10246	H-DLI-DWR--061221/1219
Improper	23-Nov-21	10	OS Command Injection	https://supp	H-DLI-DWR--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			vulnerability in debug_fcgi of D-Link DWR-932C E1 firmware allows a remote attacker to perform command injection via a crafted HTTP request. **CVE ID : CVE-2021-42784**	ortannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10246	061221/1220
hej					
hejhome_gkw-ic052					
Use of Hard-coded Credentials	26-Nov-21	7.5	HejHome GKW-IC052 IP Camera contained a hard-coded credentials vulnerability. This issue allows remote attackers to operate the IP Camera.(reboot, factory reset, snapshot etc..) **CVE ID : CVE-2021-26611**	N/A	H-HEJ-HEJH-061221/1221
Hitachi					
gms600					
Incorrect Authorization	18-Nov-21	9	Insufficient security control vulnerability in internal database access mechanism of Hitachi Energy Relion 670/650/SAM600-IO, Relion 650, GMS600, PWC600 allows attacker who successfully exploited this vulnerability, of which the product does not sufficiently restrict access to an internal database tables, could allow anybody with user credentials to bypass security controls that is enforced by the product. Consequently, exploitation may lead to unauthorized modifications on	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000059&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000058&Languag	H-HIT-GMS6-061221/1222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data/firmware, and/or to permanently disabling the product. This issue affects: Hitachi Energy Relion 670 Series 2.0 all revisions; 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.5. Hitachi Energy Relion 670/650 Series 2.1 all revisions. 2.2.0 all revisions; 2.2.4 all revisions; Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions; 2.2.5 versions prior to 2.2.5.2. Hitachi Energy Relion 650 1.0 all revisions. 1.1 all revisions; 1.2 all revisions; 1.3 versions prior to 1.3.0.8; Hitachi Energy GMS600 1.3.0; 1.3.0.1; 1.2.0. Hitachi Energy PWC600 1.0.1 version 1.0.1.4 and prior versions; 1.1.0 version 1.1.0.1 and prior versions. **CVE ID : CVE-2021-35534**	eCode=en&DocumentPartId=&Action=Launch	
pwc600					
Incorrect Authorization	18-Nov-21	9	Insufficient security control vulnerability in internal database access mechanism of Hitachi Energy Relion 670/650/SAM600-IO, Relion 650, GMS600, PWC600 allows attacker who successfully exploited this vulnerability, of which the product does not sufficiently restrict access to an internal database tables, could allow anybody with user credentials to bypass security controls that is enforced by the product.	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000059&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?	H-HIT-PWC6-061221/1223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consequently, exploitation may lead to unauthorized modifications on data/firmware, and/or to permanently disabling the product. This issue affects: Hitachi Energy Relion 670 Series 2.0 all revisions; 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.5. Hitachi Energy Relion 670/650 Series 2.1 all revisions. 2.2.0 all revisions; 2.2.4 all revisions; Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions; 2.2.5 versions prior to 2.2.5.2. Hitachi Energy Relion 650 1.0 all revisions. 1.1 all revisions; 1.2 all revisions; 1.3 versions prior to 1.3.0.8; Hitachi Energy GMS600 1.3.0; 1.3.0.1; 1.2.0. Hitachi Energy PWC600 1.0.1 version 1.0.1.4 and prior versions; 1.1.0 version 1.1.0.1 and prior versions. **CVE ID : CVE-2021-35534**	DocumentID=8DBD000058&LanguageCode=en&DocumentPartId=&Action=Launch	
relion_650					
Incorrect Authorization	18-Nov-21	9	Insufficient security control vulnerability in internal database access mechanism of Hitachi Energy Relion 670/650/SAM600-IO, Relion 650, GMS600, PWC600 allows attacker who successfully exploited this vulnerability, of which the product does not sufficiently restrict access to an internal database tables, could allow anybody with	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000059&LanguageCode=en&DocumentPartId=&Action=Launch, https://sear	H-HIT-RELI-061221/1224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user credentials to bypass security controls that is enforced by the product. Consequently, exploitation may lead to unauthorized modifications on data/firmware, and/or to permanently disabling the product. This issue affects: Hitachi Energy Relion 670 Series 2.0 all revisions; 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.5. Hitachi Energy Relion 670/650 Series 2.1 all revisions. 2.2.0 all revisions; 2.2.4 all revisions; Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions; 2.2.5 versions prior to 2.2.5.2. Hitachi Energy Relion 650 1.0 all revisions. 1.1 all revisions; 1.2 all revisions; 1.3 versions prior to 1.3.0.8; Hitachi Energy GMS600 1.3.0; 1.3.0.1; 1.2.0. Hitachi Energy PWC600 1.0.1 version 1.0.1.4 and prior versions; 1.1.0 version 1.1.0.1 and prior versions. **CVE ID : CVE-2021-35534**	ch.abb.com/library/Download.aspx?DocumentID=8DBD000058&LanguageCode=en&DocumentPartId=&Action=Launch	
Insecure Default Initialization of Resource	18-Nov-21	6.8	Insecure Boot Image vulnerability in Hitachi Energy Relion Relion 670/650/SAM600-IO series allows an attacker who manages to get access to the front network port and to cause a reboot sequences of the device may exploit the vulnerability, where there is a	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000061&LanguageCode=en&DocumentPartId=&Action=	H-HIT-RELI-061221/1225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tiny time gap during the booting process where an older version of VxWorks is loaded prior to application firmware booting, could exploit the vulnerability in the older version of VxWorks and cause a denial-of-service on the product. This issue affects: Hitachi Energy Relion 670 Series 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.3. Hitachi Energy Relion 670/650 Series 2.2.0 all revisions; 2.2.4 all revisions. Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions. **CVE ID : CVE-2021-35535**	Launch	
relion_670					
Incorrect Authorization	18-Nov-21	9	Insufficient security control vulnerability in internal database access mechanism of Hitachi Energy Relion 670/650/SAM600-IO, Relion 650, GMS600, PWC600 allows attacker who successfully exploited this vulnerability, of which the product does not sufficiently restrict access to an internal database tables, could allow anybody with user credentials to bypass security controls that is enforced by the product. Consequently, exploitation may lead to unauthorized modifications on data/firmware, and/or to permanently disabling the	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000059&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000058&LanguageCode=en&DocumentPart	H-HIT-RELI-061221/1226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			product. This issue affects: Hitachi Energy Relion 670 Series 2.0 all revisions; 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.5. Hitachi Energy Relion 670/650 Series 2.1 all revisions. 2.2.0 all revisions; 2.2.4 all revisions; Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions; 2.2.5 versions prior to 2.2.5.2. Hitachi Energy Relion 650 1.0 all revisions. 1.1 all revisions; 1.2 all revisions; 1.3 versions prior to 1.3.0.8; Hitachi Energy GMS600 1.3.0; 1.3.0.1; 1.2.0. Hitachi Energy PWC600 1.0.1 version 1.0.1.4 and prior versions; 1.1.0 version 1.1.0.1 and prior versions. **CVE ID : CVE-2021-35534**	Id=&Action=Launch	
Insecure Default Initialization of Resource	18-Nov-21	6.8	Insecure Boot Image vulnerability in Hitachi Energy Relion Relion 670/650/SAM600-IO series allows an attacker who manages to get access to the front network port and to cause a reboot sequences of the device may exploit the vulnerability, where there is a tiny time gap during the booting process where an older version of VxWorks is loaded prior to application firmware booting, could exploit the vulnerability in the older version of VxWorks and cause a denial-of-service on	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000061&LanguageCode=en&DocumentPartId=&Action=Launch	H-HIT-RELI-061221/1227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the product. This issue affects: Hitachi Energy Relion 670 Series 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.3. Hitachi Energy Relion 670/650 Series 2.2.0 all revisions; 2.2.4 all revisions. Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions. **CVE ID : CVE-2021-35535**		
relion_sam600-io					
Incorrect Authorization	18-Nov-21	9	Insufficient security control vulnerability in internal database access mechanism of Hitachi Energy Relion 670/650/SAM600-IO, Relion 650, GMS600, PWC600 allows attacker who successfully exploited this vulnerability, of which the product does not sufficiently restrict access to an internal database tables, could allow anybody with user credentials to bypass security controls that is enforced by the product. Consequently, exploitation may lead to unauthorized modifications on data/firmware, and/or to permanently disabling the product. This issue affects: Hitachi Energy Relion 670 Series 2.0 all revisions; 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.5. Hitachi Energy Relion 670/650 Series 2.1 all revisions. 2.2.0 all revisions; 2.2.4 all revisions;	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000059&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000058&LanguageCode=en&DocumentPartId=&Action=Launch	H-HIT-RELI-061221/1228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions; 2.2.5 versions prior to 2.2.5.2. Hitachi Energy Relion 650 1.0 all revisions. 1.1 all revisions; 1.2 all revisions; 1.3 versions prior to 1.3.0.8; Hitachi Energy GMS600 1.3.0; 1.3.0.1; 1.2.0. Hitachi Energy PWC600 1.0.1 version 1.0.1.4 and prior versions; 1.1.0 version 1.1.0.1 and prior versions. **CVE ID : CVE-2021-35534**		
Insecure Default Initialization of Resource	18-Nov-21	6.8	Insecure Boot Image vulnerability in Hitachi Energy Relion Relion 670/650/SAM600-IO series allows an attacker who manages to get access to the front network port and to cause a reboot sequences of the device may exploit the vulnerability, where there is a tiny time gap during the booting process where an older version of VxWorks is loaded prior to application firmware booting, could exploit the vulnerability in the older version of VxWorks and cause a denial-of-service on the product. This issue affects: Hitachi Energy Relion 670 Series 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.3. Hitachi Energy Relion 670/650 Series 2.2.0 all revisions; 2.2.4 all revisions. Hitachi Energy Relion	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000061&LanguageCode=en&DocumentPartId=&Action=Launch	H-HIT-RELI-061221/1229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			670/650/SAM600-IO 2.2.1 all revisions. **CVE ID : CVE-2021-35535**		
Huawei					
cloudengine_5800					
Improper Privilege Management	23-Nov-21	7.2	There is a privilege escalation vulnerability in CloudEngine 5800 V200R020C00SPC600. Due to lack of privilege restrictions, an authenticated local attacker can perform specific operation to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege. **CVE ID : CVE-2021-39976**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211103-01-privilege-en	H-HUA-CLOU-061221/1230
ecns280_td					
Exposure of Sensitive Information to an Unauthorized Actor	23-Nov-21	2.1	There is an information leakage vulnerability in FusionCompute 6.5.1, eCNS280_TD V100R005C00 and V100R005C10. Due to the improperly storage of specific information in the log file, the attacker can obtain the information when a user logs in to the device. Successful exploit may cause the information leak. **CVE ID : CVE-2021-37036**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210818-01-informationleak-en	H-HUA-ECNS-061221/1231
Out-of-bounds Read	29-Nov-21	6.8	Some Huawei products use the OpenHpi software for hardware management. A function that parses data returned by OpenHpi contains an out-of-bounds read vulnerability that could lead	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211124-	H-HUA-ECNS-061221/1232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a denial of service. Affected product versions include: eCNS280_TD V100R005C10; eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. **CVE ID : CVE-2021-39995**	03-dos-en	
ese620x_vess					
Out-of-bounds Read	29-Nov-21	6.8	Some Huawei products use the OpenHpi software for hardware management. A function that parses data returned by OpenHpi contains an out-of-bounds read vulnerability that could lead to a denial of service. Affected product versions include: eCNS280_TD V100R005C10; eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. **CVE ID : CVE-2021-39995**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211124-03-dos-en	H-HUA-ESE6-061221/1233
imaster_nce-fabric					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	3.5	There is a XSS injection vulnerability in iMaster NCE-Fabric V100R019C10. A module of the client does not verify the input sufficiently. Attackers can exploit this vulnerability by modifying input after logging onto the client. This may compromise the normal service of the client. **CVE ID : CVE-2021-22410**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210324-01-xss-en	H-HUA-IMAS-061221/1234
ips_module					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of a Broken or Risky Cryptographic Algorithm	23-Nov-21	4.3	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a module. Attackers can exploit this vulnerability by capturing and analyzing the messages between devices to obtain information. This can lead to information leak.Affected product versions include: IPS Module V500R005C00SPC100, V500R005C00SPC200; NGFW Module V500R005C00SPC100, V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; USG9500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-infomationleak-en	H-HUA-IPS_-061221/1235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22356		
ngfw_module					
Use of a Broken or Risky Cryptographic Algorithm	23-Nov-21	4.3	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a module. Attackers can exploit this vulnerability by capturing and analyzing the messages between devices to obtain information. This can lead to information leak.Affected product versions include: IPS Module V500R005C00SPC100, V500R005C00SPC200; NGFW Module V500R005C00SPC100, V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; USG9500 V500R001C30SPC200, V500R001C30SPC600,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-infomationleak-en	H-HUA-NGFW-061221/1236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200. **CVE ID : CVE-2021-22356**		
secospace_usg6300					
Use of a Broken or Risky Cryptographic Algorithm	23-Nov-21	4.3	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a module. Attackers can exploit this vulnerability by capturing and analyzing the messages between devices to obtain information. This can lead to information leak.Affected product versions include: IPS Module V500R005C00SPC100, V500R005C00SPC200; NGFW Module V500R005C00SPC100, V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200;	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-infomationleak-en	H-HUA-SECO-061221/1237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			USG9500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200. **CVE ID : CVE-2021-22356**		
secospace_usg6500					
Use of a Broken or Risky Cryptographic Algorithm	23-Nov-21	4.3	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a module. Attackers can exploit this vulnerability by capturing and analyzing the messages between devices to obtain information. This can lead to information leak.Affected product versions include: IPS Module V500R005C00SPC100, V500R005C00SPC200; NGFW Module V500R005C00SPC100, V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-infomationleak-en	H-HUA-SECO-061221/1238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; USG9500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200. **CVE ID : CVE-2021-22356**		
secospace_usg6600					
Use of a Broken or Risky Cryptographic Algorithm	23-Nov-21	4.3	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a module. Attackers can exploit this vulnerability by capturing and analyzing the messages between devices to obtain information. This can lead to information leak.Affected product versions include: IPS Module V500R005C00SPC100, V500R005C00SPC200; NGFW Module V500R005C00SPC100, V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200;	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-infomationleak-en	H-HUA-SECO-061221/1239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; USG9500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200. **CVE ID : CVE-2021-22356**		
usg9500					
Use of a Broken or Risky Cryptographic Algorithm	23-Nov-21	4.3	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a module. Attackers can exploit this vulnerability by capturing and analyzing the messages between devices to obtain information. This can lead to information leak.Affected product versions include: IPS Module V500R005C00SPC100, V500R005C00SPC200; NGFW Module V500R005C00SPC100, V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-infomationleak-en	H-HUA-USG9-061221/1240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; USG9500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200. **CVE ID : CVE-2021-22356**		
Intel					
7265					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-7265-061221/1241
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-7265-061221/1242
Improper	17-Nov-21	4.6	Insecure inherited	https://ww	H-INT-7265-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Preservation of Permissions			permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	061221/1243
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-7265-061221/1244
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-7265-061221/1245
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-7265-061221/1246
Out-of-bounds	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R)	https://www.intel.com/	H-INT-7265-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	content/www/us/en/security-center/advisory/intel-sa-00509.html	061221/1247
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-7265-061221/1248
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-7265-061221/1249
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-7265-061221/1250
ac1550					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R)	https://www.intel.com/	H-INT-AC15-061221/1251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	content/www/us/en/security-center/advisory/intel-sa-00509.html	
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC15-061221/1252
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC15-061221/1253
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC15-061221/1254
Improper Input	17-Nov-21	6.8	Improper input validation in software for some Intel(R)	https://www.intel.com/	H-INT-AC15-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	content/www/us/en/security-center/advisory/intel-sa-00509.html	061221/1255
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC15-061221/1256
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC15-061221/1257
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC15-061221/1258
Improper Verification of Cryptographi	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R)	https://www.intel.com/content/www/us/en/security-	H-INT-AC15-061221/1259

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c Signature			products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	center/advisory/intel-sa-00540.html	
ac_3165					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1260
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1261
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1262
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi	https://www.intel.com/content/ww	H-INT-AC_3-061221/1263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	w/us/en/security-center/advisory/intel-sa-00509.html	
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1264
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1265
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1266
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows	https://www.intel.com/content/www/us/en/se	H-INT-AC_3-061221/1267

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	curity-center/advisory/intel-sa-00509.html	
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1268
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1269
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_3-061221/1270
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_3-061221/1271

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	00540.html	
ac_3168					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1272
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1273
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1274
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version	https://www.intel.com/content/www/us/en/security-	H-INT-AC_3-061221/1275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	center/advisory/intel-sa-00509.html	
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1276
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1277
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1278
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-AC_3-061221/1279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	ory/intel-sa-00509.html	
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1280
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_3-061221/1281
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_3-061221/1282
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_3-061221/1283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2021-0152**		
ac_7265					
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_7-061221/1284
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_7-061221/1285
ac_8260					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1286
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an	https://www.intel.com/content/www/us/en/security-	H-INT-AC_8-061221/1287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	center/advisory/intel-sa-00509.html	
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1288
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1289
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1290
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable	https://www.intel.com/content/www/us/en/security-	H-INT-AC_8-061221/1291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	center/advisory/intel-sa-00509.html	
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1292
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1293
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1294
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_8-061221/1295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2021-0082**	00509.html	
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_8-061221/1296
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_8-061221/1297
ac_8265					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1298
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-AC_8-061221/1299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	ory/intel-sa-00509.html	
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1300
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1301
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1302
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-AC_8-061221/1303

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent access. **CVE ID : CVE-2021-0071**	ory/intel-sa-00509.html	
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1304
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1305
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_8-061221/1306
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_8-061221/1307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0082	00509.html	
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_8-061221/1308
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_8-061221/1309
ac_9260					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1310
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_9-061221/1311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via adjacent access. **CVE ID : CVE-2021-0063**	00509.html	
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1312
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1313
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1314
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_9-061221/1315

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent access. **CVE ID : CVE-2021-0071**	00509.html	
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1316
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1317
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1318
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_9-061221/1319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0082	00509.html	
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_9-061221/1320
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_9-061221/1321
ac_9461					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1322
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_9-061221/1323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via adjacent access. **CVE ID : CVE-2021-0063**	00509.html	
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1324
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1325
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1326
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_9-061221/1327

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent access. **CVE ID : CVE-2021-0071**	00509.html	
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1328
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1329
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1330
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_9-061221/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0082	00509.html	
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_9-061221/1332
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_9-061221/1333
ac_9462					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1334
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_9-061221/1335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via adjacent access. **CVE ID : CVE-2021-0063**	00509.html	
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1336
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1337
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1338
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_9-061221/1339

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent access. **CVE ID : CVE-2021-0071**	00509.html	
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1340
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1341
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1342
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_9-061221/1343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0082	00509.html	
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_9-061221/1344
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_9-061221/1345
ac_9560					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1346
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_9-061221/1347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via adjacent access. **CVE ID : CVE-2021-0063**	00509.html	
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1348
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1349
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1350
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_9-061221/1351

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent access. **CVE ID : CVE-2021-0071**	00509.html	
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1352
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1353
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AC_9-061221/1354
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AC_9-061221/1355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0082	00509.html	
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_9-061221/1356
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AC_9-061221/1357
atom_c3000					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-ATOM-061221/1358
atom_x5-e3930					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-ATOM-061221/1359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access. **CVE ID : CVE-2021-0146**	00528.html	
atom_x5-e3940					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-ATOM-061221/1360
atom_x7-e3950					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-ATOM-061221/1361
ax1650					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX16-061221/1362
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an	https://www.intel.com/content/www/us/en/security-	H-INT-AX16-061221/1363

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	center/advisory/intel-sa-00509.html	
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX16-061221/1364
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX16-061221/1365
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX16-061221/1366
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an	https://www.intel.com/content/www/us/en/security-	H-INT-AX16-061221/1367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	center/advisory/intel-sa-00509.html	
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX16-061221/1368
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AX16-061221/1369
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AX16-061221/1370
ax1675					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-AX16-061221/1371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	ory/intel-sa-00509.html	
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX16-061221/1372
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX16-061221/1373
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX16-061221/1374
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-AX16-061221/1375

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	ory/intel-sa-00509.html	
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX16-061221/1376
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX16-061221/1377
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AX16-061221/1378
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AX16-061221/1379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2021-0152**		
ax200					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1380
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1381
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1382
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-AX20-061221/1383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	ory/intel-sa-00509.html	
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1384
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1385
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1386
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AX20-061221/1387

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	00509.html	
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1388
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1389
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AX20-061221/1390
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AX20-061221/1391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0152		
ax201					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1392
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1393
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1394
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AX20-061221/1395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	00509.html	
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1396
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1397
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1398
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-AX20-061221/1399

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure via adjacent access. **CVE ID : CVE-2021-0078**	00509.html	
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1400
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX20-061221/1401
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AX20-061221/1402
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AX20-061221/1403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ax210					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX21-061221/1404
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX21-061221/1405
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX21-061221/1406
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX21-061221/1407

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0065		
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX21-061221/1408
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX21-061221/1409
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX21-061221/1410
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX21-061221/1411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0078		
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX21-061221/1412
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	H-INT-AX21-061221/1413
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AX21-061221/1414
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	H-INT-AX21-061221/1415
celeron_j1750					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1416
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1417
celeron_j1800					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1418
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1419
celeron_j1850					
Improper Privilege	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime	https://www.intel.com/	H-INT-CELE-061221/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	content/www/us/en/security-center/advisory/intel-sa-00528.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1421
celeron_j1900					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1422
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1423
celeron_j3060					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an	https://www.intel.com/content/www/us/en/se	H-INT-CELE-061221/1424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	curity-center/advisory/intel-sa-00528.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1425
celeron_j3160					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1426
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1427
celeron_j3355					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CELE-061221/1428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via physical access. **CVE ID : CVE-2021-0146**	ory/intel-sa-00528.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1429
celeron_j3355e					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1430
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1431
celeron_j3455					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1432

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0146		
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1433
celeron_j3455e					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1434
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1435
celeron_j4005					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1437
celeron_j4025					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1438
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1439
celeron_j4105					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1440
Improper Input	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK	https://www.intel.com/	H-INT-CELE-061221/1441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	content/www/us/en/security-center/advisory/intel-sa-00548.html	
celeron_j4125					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1442
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1443
celeron_j6412					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1444
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may	https://www.intel.com/content/www/us/en/se	H-INT-CELE-061221/1445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	curity-center/advisory/intel-sa-00548.html	
celeron_j6413					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1446
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1447
celeron_n2805					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1448
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CELE-061221/1449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1450
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1451
celeron_n2806					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1452
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1453
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-CELE-061221/1454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1455
celeron_n2807					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1456
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1457
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CELE-061221/1458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1459
celeron_n2808					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1460
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1461
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1462
Improper Input	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK	https://www.intel.com/	H-INT-CELE-061221/1463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	content/www/us/en/security-center/advisory/intel-sa-00548.html	
celeron_n2810					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1464
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1465
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1466
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CELE-061221/1467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	ory/intel-sa-00548.html	
celeron_n2815					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1468
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1469
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1470
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1471
celeron_n2820					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1472
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1473
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1474
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1475
celeron_n2830					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an	https://www.intel.com/content/www/us/en/se	H-INT-CELE-061221/1476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	curity-center/advisory/intel-sa-00528.html	
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1477
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1478
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1479
celeron_n2840					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0146		
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1481
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1482
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1483
celeron_n2910					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1484
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-CELE-061221/1485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1486
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1487
celeron_n2920					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1488
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CELE-061221/1489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1490
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1491
celeron_n2930					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1492
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1493
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-CELE-061221/1494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1495
celeron_n2940					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1496
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1497
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CELE-061221/1498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1499
celeron_n3000					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1500
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1501
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1502
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for	https://www.intel.com/content/ww	H-INT-CELE-061221/1503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w/us/en/security-center/advisory/intel-sa-00548.html	
celeron_n3010					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1504
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1505
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1506
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CELE-061221/1507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0186	00548.html	
celeron_n3050					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1508
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1509
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1510
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1511
celeron_n3060					
Improper Privilege	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime	https://www.intel.com/	H-INT-CELE-061221/1512

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	content/www/us/en/security-center/advisory/intel-sa-00528.html	
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1513
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1514
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1515
celeron_n3150					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CELE-061221/1516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via physical access. **CVE ID : CVE-2021-0146**	ory/intel-sa-00528.html	
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1517
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1518
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1519
celeron_n3160					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1520
Improper	17-Nov-21	4.6	Insufficient control flow	https://ww	H-INT-CELE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/1521
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1522
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1523
celeron_n3350					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1524
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially	https://www.intel.com/content/www/us/en/security-	H-INT-CELE-061221/1525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1526
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1527
celeron_n3350e					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1528
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1529
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	H-INT-CELE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/1530
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1531
celeron_n3450					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1532
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1533
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-	H-INT-CELE-061221/1534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2021-0158**	center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1535
celeron_n4000					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1536
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1537
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1538
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	H-INT-CELE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	061221/1539
celeron_n4020					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1540
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1541
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1542
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to	https://www.intel.com/content/www/us/en/security-	H-INT-CELE-061221/1543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	center/advisory/intel-sa-00548.html	
celeron_n4100					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1544
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1545
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1546
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1547
celeron_n4120					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1548
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1549
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1550
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1551
celeron_n4500					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an	https://www.intel.com/content/www/us/en/se	H-INT-CELE-061221/1552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	curity-center/advisory/intel-sa-00528.html	
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1553
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1554
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1555
celeron_n4505					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0146		
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1557
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1558
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1559
celeron_n5100					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1560
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-CELE-061221/1561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1562
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1563
celeron_n5105					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1564
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CELE-061221/1565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1566
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1567
celeron_n6210					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1568
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1569
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-CELE-061221/1570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1571
celeron_n6211					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-CELE-061221/1572
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CELE-061221/1573
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CELE-061221/1574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CELE-061221/1575
core_i3-1000g1					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1576
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1577
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1578
core_i3-1000g4					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-CORE-061221/1579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1580
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1581
core_i3-1005g1					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1582
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1584
core_i3-10100					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1585
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1586
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1587
core_i3-10100e					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/1588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1589
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1590
core_i3-10100f					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1591
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1592
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	061221/1593
core_i3-10100t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1594
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1595
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1596
core_i3-10100te					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially	https://www.intel.com/content/www/us/en/security-	H-INT-CORE-061221/1597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1598
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1599
core_i3-10100y					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1600
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1601
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/1602
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1603
core_i3-10105					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1604
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1605
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	00548.html	
core_i3-10105f					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1607
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1608
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1609
core_i3-10105t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1610
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/1611
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1612
core_i3-10110u					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1613
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1614
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1616
core_i3-10110y					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1617
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1618
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1619
Improper Input	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK	https://www.intel.com/	H-INT-CORE-061221/1620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	content/www/us/en/security-center/advisory/intel-sa-00548.html	
core_i3-10300					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1621
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1622
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1623
core_i3-10300t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1625
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1626
core_i3-10305					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1627
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1628
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for	https://www.intel.com/content/ww	H-INT-CORE-061221/1629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w/us/en/security-center/advisory/intel-sa-00548.html	
core_i3-10305t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1630
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1631
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1632
core_i3-10320					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1634
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1635
core_i3-10325					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1636
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1637
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/1638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	curity-center/advisory/intel-sa-00548.html	
core_i3-11100he					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1639
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1640
core_i3-1110g4					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1641
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1643
core_i3-1115g4					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1644
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1645
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1646
core_i3-1115g4e					
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-CORE-061221/1647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1648
core_i3-1115gre					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1649
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1650
core_i3-1120g4					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	ory/intel-sa-00533.html	
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1652
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1653
core_i3-1125g4					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1654
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1655
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/1656
core_i3-7020u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1657
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1658
core_i3-7100					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1659
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-	H-INT-CORE-061221/1660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2021-0158**	center/advisory/intel-sa-00562.html	
core_i3-7100e					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1661
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1662
core_i3-7100h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1663
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1664
core_i3-7100t					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1665
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1666
core_i3-7100u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1667
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1668
core_i3-7101e					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/1669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1670
core_i3-7101te					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1671
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1672
core_i3-7102e					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1674
core_i3-7130u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1675
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1676
core_i3-7167u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1677
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/1678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
core_i3-7300					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1679
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1680
core_i3-7300t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1681
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i3-7320					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1683
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1684
core_i3-7350k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1685
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1686
core_i3-8100					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-CORE-061221/1687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1688
core_i3-8100b					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1689
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1690
core_i3-8100h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1692
core_i3-8100t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1693
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1694
core_i3-8109u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1695
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-CORE-061221/1696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
core_i3-8130u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1697
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1698
core_i3-8140u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1699
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00562.html	
core_i3-8145u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1701
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1702
core_i3-8145ue					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1703
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1704
core_i3-8300					
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/1705
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1706
core_i3-8300t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1707
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1708
core_i3-8350k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1710
core_i5-10200h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1711
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1712
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1713
core_i5-10210u					
Incorrect Authorizatio	17-Nov-21	2.1	Improper access control in some Intel(R)	https://www.intel.com/	H-INT-CORE-061221/1714

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	content/www/us/en/security-center/advisory/intel-sa-00533.html	
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1715
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1716
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1717
core_i5-10210y					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	ory/intel-sa-00533.html	
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1719
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1720
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1721
core_i5-10300h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1722
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-CORE-061221/1723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1724
core_i5-1030g4					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1725
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1726
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0186	00548.html	
core_i5-1030g7					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1728
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1729
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1730
core_i5-10310u					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1731
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-CORE-061221/1732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1733
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1734
core_i5-10310y					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1735
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1737
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1738
core_i5-1035g1					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1739
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1740
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for	https://www.intel.com/content/ww	H-INT-CORE-061221/1741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w/us/en/security-center/advisory/intel-sa-00548.html	
core_i5-1035g4					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1742
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1743
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1744
core_i5-1035g7					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1746
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1747
core_i5-1038ng7					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1748
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1749
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/1750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	curity-center/advisory/intel-sa-00548.html	
core_i5-10400					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1751
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1752
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1753
core_i5-10400f					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1754

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1755
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1756
core_i5-10400h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1757
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1758
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	ory/intel-sa-00548.html	
core_i5-10400t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1760
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1761
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1762
core_i5-10500					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1763
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/1764
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1765
core_i5-10500e					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1766
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1767
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0186	00548.html	
core_i5-10500h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1769
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1770
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1771
core_i5-10500t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1772
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-CORE-061221/1773

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1774
core_i5-10500te					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1775
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1776
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-10505					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1778
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1779
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1780
core_i5-10600					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1781
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/1782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1783
core_i5-10600k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1784
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1785
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1786
core_i5-10600kf					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1787
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1788
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1789
core_i5-10600t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1790
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-	H-INT-CORE-061221/1791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2021-0158**	center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1792
core_i5-10610u					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1793
core_i5-11260h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1794
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-11300h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1796
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1797
core_i5-1130g7					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1798
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1799
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-CORE-061221/1800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
core_i5-11320h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1801
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1802
core_i5-1135g7					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1803
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1805
core_i5-11400					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1806
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1807
core_i5-11400f					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1808
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-CORE-061221/1809

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
core_i5-11400h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1810
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1811
core_i5-11400t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1812
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
core_i5-1140g7					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1814
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1815
core_i5-1145g7					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1816
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1817
core_i5-1145g7e					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1818
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1819
core_i5-1145gre					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1820
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1821
core_i5-11500					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/1822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1823
core_i5-11500h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1824
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1825
core_i5-11500he					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1827
core_i5-11500t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1828
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1829
core_i5-1155g7					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1830
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/1831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
core_i5-11600					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1832
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1833
core_i5-11600k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1834
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-11600kf					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1836
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1837
core_i5-11600t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1838
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1839
core_i5-7200u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-CORE-061221/1840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1841
core_i5-7260u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1842
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1843
core_i5-7267u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1845
core_i5-7287u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1846
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1847
core_i5-7300hq					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1848
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-CORE-061221/1849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
core_i5-7300u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1850
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1851
core_i5-7360u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1852
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00562.html	
core_i5-7400					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1854
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1855
core_i5-7400t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1856
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1857
core_i5-7440eq					
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/1858
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1859
core_i5-7440hq					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1860
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1861
core_i5-7442eq					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1863
core_i5-7500					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1864
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1865
core_i5-7500t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1866
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-CORE-061221/1867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
core_i5-7600					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1868
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1869
core_i5-7600k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1870
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
core_i5-7600t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1872
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1873
core_i5-7640x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1874
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1875
core_i5-7y54					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1876
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1877
core_i5-7y57					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1878
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1879
core_i5-8200y					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/1880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1881
core_i5-8210y					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1882
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1883
core_i5-8250u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1885
core_i5-8257u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1886
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1887
core_i5-8259u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1888
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/1889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
core_i5-8260u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1890
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1891
core_i5-8265u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1892
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-8269u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1894
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1895
core_i5-8279u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1896
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1897
core_i5-8300h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-CORE-061221/1898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1899
core_i5-8305g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1900
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1901
core_i5-8310y					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1903
core_i5-8350u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1904
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1905
core_i5-8365u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1906
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-CORE-061221/1907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
core_i5-8365ue					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1908
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1909
core_i5-8400					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1910
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00562.html	
core_i5-8400b					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1912
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1913
core_i5-8400h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1914
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1915
core_i5-8400t					
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/1916
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1917
core_i5-8500					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1918
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1919
core_i5-8500b					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1921
core_i5-8500t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1922
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1923
core_i5-8600					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1924
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-CORE-061221/1925

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
core_i5-8600k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1926
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1927
core_i5-8600t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1928
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
core_i7-10510u					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1930
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1931
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1932
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1933
core_i7-10510y					
Incorrect	17-Nov-21	2.1	Improper access control in	https://ww	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	061221/1934
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1935
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1936
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1937
core_i7-1060g7					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially	https://www.intel.com/content/www/us/en/security-	H-INT-CORE-061221/1938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1939
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1940
core_i7-10610u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1941
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1942
Improper Input	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK	https://www.intel.com/	H-INT-CORE-061221/1943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	content/www/us/en/security-center/advisory/intel-sa-00548.html	
core_i7-1065g7					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1944
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1945
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1946
core_i7-1068ng7					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1948
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1949
core_i7-10700					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1950
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1951
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for	https://www.intel.com/content/ww	H-INT-CORE-061221/1952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w/us/en/security-center/advisory/intel-sa-00548.html	
core_i7-10700e					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1953
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1954
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1955
core_i7-10700f					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/1956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1957
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1958
core_i7-10700k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1959
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1960
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/1961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	curity-center/advisory/intel-sa-00548.html	
core_i7-10700kf					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1962
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1963
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1964
core_i7-10700t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1965

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1966
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1967
core_i7-10700te					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1968
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1969
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/1970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	ory/intel-sa-00548.html	
core_i7-10710u					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1971
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1972
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1973
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1974
core_i7-10750h					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1975
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1976
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1977
core_i7-10810u					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1978
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/1979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1980
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1981
core_i7-10850h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1982
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1983
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	061221/1984
core_i7-10870h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1985
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1986
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1987
core_i7-10875h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially	https://www.intel.com/content/www/us/en/security-	H-INT-CORE-061221/1988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1989
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/1990
core_i7-11370h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1991
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1992
core_i7-11375h					
Improper	17-Nov-21	4.6	Insufficient control flow	https://ww	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/1993
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1994
core_i7-11390h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1995
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1996
core_i7-11600h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially	https://www.intel.com/content/www/us/en/security-	H-INT-CORE-061221/1997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/1998
core_i7-1160g7					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/1999
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2000
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2001
core_i7-1165g7					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/2002
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2003
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2004
core_i7-11700					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2005
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/2006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
core_i7-11700f					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2007
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2008
core_i7-11700k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2009
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-11700kf					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2011
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2012
core_i7-11700t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2013
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2014
core_i7-11800h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-CORE-061221/2015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2016
core_i7-1180g7					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2017
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2018
core_i7-11850h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/2019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2020
core_i7-11850he					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2021
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2022
core_i7-1185g7					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-CORE-061221/2023
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-CORE-061221/2024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2025
core_i7-1185g7e					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2026
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2027
core_i7-1185gre					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/2028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2029
core_i7-1195g7					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2030
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2031
core_i7-3820					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2032
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-CORE-061221/2033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
core_i7-3920xm					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2034
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2035
core_i7-3930k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2036
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/2037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
core_i7-3940xm					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2038
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2039
core_i7-3960x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2040
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2041
core_i7-3970x					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2042
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2043
core_i7-4820k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2044
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2045
core_i7-4930k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/2046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2047
core_i7-4930mx					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2048
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2049
core_i7-4940mx					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2051
core_i7-4960x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2052
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2053
core_i7-5820k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2054
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/2055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
core_i7-5930k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2056
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2057
core_i7-5960x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2058
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-6800k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2060
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2061
core_i7-6850k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2062
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2063
core_i7-6900k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-CORE-061221/2064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2065
core_i7-6950x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2066
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2067
core_i7-7500u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/2068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2069
core_i7-7560u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2070
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2071
core_i7-7567u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2072
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-CORE-061221/2073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
core_i7-7600u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2074
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2075
core_i7-7660u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2076
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/2077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00562.html	
core_i7-7700					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2078
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2079
core_i7-7700hq					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2080
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2081
core_i7-7700k					
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/2082
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2083
core_i7-7700t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2084
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2085
core_i7-7740x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/2086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2087
core_i7-7800x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2088
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2089
core_i7-7820eq					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2090
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-CORE-061221/2091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
core_i7-7820hk					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2092
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2093
core_i7-7820hq					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2094
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/2095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
core_i7-7820x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2096
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2097
core_i7-7920hq					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2098
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2099
core_i7-7y75					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2100
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2101
core_i7-8086k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2102
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2103
core_i7-8500y					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/2104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2105
core_i7-8550u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2106
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2107
core_i7-8557u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2109
core_i7-8559u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2110
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2111
core_i7-8565u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2112
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/2113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
core_i7-8569u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2114
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2115
core_i7-8650u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2116
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-8665u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2118
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2119
core_i7-8665ue					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2120
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2121
core_i7-8700					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-CORE-061221/2122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2123
core_i7-8700b					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2124
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2125
core_i7-8700k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/2126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2127
core_i7-8700t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2128
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2129
core_i7-8705g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2130
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-CORE-061221/2131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
core_i7-8706g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2132
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2133
core_i7-8709g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2134
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/2135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00562.html	
core_i7-8750h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2136
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2137
core_i7-8809g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2138
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2139
core_i7-8850h					
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/2140
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2141
core_i7-9800x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2142
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2143
core_i9-10850k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/2144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2145
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/2146
core_i9-10885h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2147
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2148
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for	https://www.intel.com/content/ww	H-INT-CORE-061221/2149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w/us/en/security-center/advisory/intel-sa-00548.html	
core_i9-10900					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2150
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2151
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/2152
core_i9-10900e					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/2153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2154
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/2155
core_i9-10900f					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2156
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2157
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/2158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	curity-center/advisory/intel-sa-00548.html	
core_i9-10900k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2159
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2160
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/2161
core_i9-10900kf					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2162

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2163
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/2164
core_i9-10900t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2165
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2166
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/2167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	ory/intel-sa-00548.html	
core_i9-10900te					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2168
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2169
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/2170
core_i9-10900x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2171
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	061221/2172
core_i9-10920x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2173
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2174
core_i9-10940x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2175
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/2176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
core_i9-10980hk					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2177
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2178
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-CORE-061221/2179
core_i9-10980xe					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2180
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-CORE-061221/2181

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
core_i9-11900					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2182
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2183
core_i9-11900f					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2184
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-CORE-061221/2185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
core_i9-11900h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2186
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2187
core_i9-11900k					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2188
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2189
core_i9-11900kf					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2190
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2191
core_i9-11900t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2192
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2193
core_i9-11950h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/2194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2195
core_i9-11980hk					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2196
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2197
core_i9-7900x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2199
core_i9-7920x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2200
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2201
core_i9-7940x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2202
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-CORE-061221/2203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
core_i9-7960x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2204
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2205
core_i9-7980xe					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2206
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i9-8950hk					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2208
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2209
core_i9-9820x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2210
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2211
core_i9-9900x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-CORE-061221/2212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2213
core_i9-9920x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2214
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2215
core_i9-9940x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-CORE-061221/2216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2217
core_i9-9960x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2218
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2219
core_i9-9980xe					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-CORE-061221/2220
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-CORE-061221/2221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
ethernet_connection_x540					
Improper Input Validation	17-Nov-21	4.9	Improper input validation in the Intel(R) Ethernet ixgbe driver for Linux before version 3.17.3 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33098**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00555.html	H-INT-ETHE-061221/2222
ethernet_connection_x550					
Improper Input Validation	17-Nov-21	4.9	Improper input validation in the Intel(R) Ethernet ixgbe driver for Linux before version 3.17.3 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33098**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00555.html	H-INT-ETHE-061221/2223
ethernet_connection_x557					
Improper Input Validation	17-Nov-21	4.9	Improper input validation in the Intel(R) Ethernet ixgbe driver for Linux before version 3.17.3 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33098**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00555.html	H-INT-ETHE-061221/2224
ethernet_controller_v710-at2					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2	https://www.intel.com/content/www/us/en/se	H-INT-ETHE-061221/2225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	curity-center/advisory/intel-sa-00554.html	
ethernet_controller_x710-am2					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-061221/2226
ethernet_controller_x710-at2					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-061221/2227
ethernet_controller_x710-bm2					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-061221/2228
ethernet_controller_x710-tm4					
Out-of-	17-Nov-21	4.6	Out-of-bounds write in the	https://ww	H-INT-ETHE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	061221/2229
ethernet_controller_xl710-am1					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-061221/2230
ethernet_controller_xl710-am2					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-061221/2231
ethernet_controller_xl710-bm1					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-061221/2232

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ethernet_controller_xl710-bm2					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-061221/2233
ethernet_controller_xxv710-am1					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-061221/2234
ethernet_controller_xxv710-am2					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-061221/2235
ethernet_network_controller_e810-cam1					
N/A	17-Nov-21	2.1	Protection mechanism failure in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to enable a denial of service via local	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-ETHE-061221/2236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access. **CVE ID : CVE-2021-0197**	00554.html	
Incorrect Authorization	17-Nov-21	2.1	Improper access control in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to potentially enable a denial of service via local access. **CVE ID : CVE-2021-0198**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-061221/2237
Improper Input Validation	17-Nov-21	2.1	Improper input validation in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.6.0.6 may allow a privileged user to potentially enable a denial of service via local access. **CVE ID : CVE-2021-0199**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-061221/2238
ethernet_network_controller_e810-cam2					
N/A	17-Nov-21	2.1	Protection mechanism failure in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to enable a denial of service via local access. **CVE ID : CVE-2021-0197**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-071221/2239
Incorrect Authorization	17-Nov-21	2.1	Improper access control in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to potentially enable a denial of service via local access. **CVE ID : CVE-2021-0198**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-071221/2240
Improper Input	17-Nov-21	2.1	Improper input validation in the firmware for the Intel(R)	https://www.intel.com/	H-INT-ETHE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Ethernet Network Controller E810 before version 1.6.0.6 may allow a privileged user to potentially enable a denial of service via local access. **CVE ID : CVE-2021-0199**	content/www/us/en/security-center/advisory/intel-sa-00554.html	071221/2241
ethernet_network_controller_e810-xxvam2					
N/A	17-Nov-21	2.1	Protection mechanism failure in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to enable a denial of service via local access. **CVE ID : CVE-2021-0197**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-071221/2242
Incorrect Authorization	17-Nov-21	2.1	Improper access control in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to potentially enable a denial of service via local access. **CVE ID : CVE-2021-0198**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-071221/2243
Improper Input Validation	17-Nov-21	2.1	Improper input validation in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.6.0.6 may allow a privileged user to potentially enable a denial of service via local access. **CVE ID : CVE-2021-0199**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	H-INT-ETHE-071221/2244
jhl6240					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow	https://www.intel.com/content/www/us/en/security-	H-INT-JHL6-071221/2245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	center/advisory/intel-sa-00533.html	
jhl6340					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-JHL6-071221/2246
jhl6540					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-JHL6-071221/2247
jhl7340					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-JHL7-071221/2248
jhl7440					
Incorrect Authorizatio	17-Nov-21	2.1	Improper access control in some Intel(R)	https://www.intel.com/	H-INT-JHL7-071221/2249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	content/www/us/en/security-center/advisory/intel-sa-00533.html	
jhl7540					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-JHL7-071221/2250
jhl8440					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-JHL8-071221/2251
jhl8540					
Incorrect Authorization	17-Nov-21	2.1	Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0110**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.html	H-INT-JHL8-071221/2252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nuc10i3fn					
Incorrect Default Permissions	17-Nov-21	7.2	Incorrect default permissionsin the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC10i3FN, NUC10i5FN, NUC10i7FN before version 1.78.2.0.7 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33090**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	H-INT-NUC1-071221/2253
nuc10i5fn					
Incorrect Default Permissions	17-Nov-21	7.2	Incorrect default permissionsin the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC10i3FN, NUC10i5FN, NUC10i7FN before version 1.78.2.0.7 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33090**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	H-INT-NUC1-071221/2254
nuc10i7fn					
Incorrect Default Permissions	17-Nov-21	7.2	Incorrect default permissionsin the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC10i3FN, NUC10i5FN, NUC10i7FN before version 1.78.2.0.7 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33090**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	H-INT-NUC1-071221/2255
nuc7i3dn					
Improper	17-Nov-21	4.6	Improper authentication in	https://ww	H-INT-NUC7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC7i3DN, NUC7i5DN, NUC7i7DN before version 1.78.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0096**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	071221/2256
nuc7i5dn					
Improper Authentication	17-Nov-21	4.6	Improper authentication in the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC7i3DN, NUC7i5DN, NUC7i7DN before version 1.78.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0096**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	H-INT-NUC7-071221/2257
nuc7i7dn					
Improper Authentication	17-Nov-21	4.6	Improper authentication in the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC7i3DN, NUC7i5DN, NUC7i7DN before version 1.78.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0096**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	H-INT-NUC7-071221/2258
nuc_10_performance_kit_nuc10i3fnh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-NUC_-071221/2259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-33086	ory/intel-sa-00567.html	
nuc_10_performance_kit_nuc10i3fnhf					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2260
nuc_10_performance_kit_nuc10i3fnhfa					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2261
nuc_10_performance_kit_nuc10i3fnhja					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2262
nuc_10_performance_kit_nuc10i3fnk					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nuc_10_performance_kit_nuc10i5fnh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2264
nuc_10_performance_kit_nuc10i5fnhca					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2265
nuc_10_performance_kit_nuc10i5fnhf					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2266
nuc_10_performance_kit_nuc10i5fnhj					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2267
nuc_10_performance_kit_nuc10i5fnhja					
Out-of-	17-Nov-21	4.9	Out-of-bounds write in	https://ww	H-INT-NUC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	071221/2268
nuc_10_performance_kit_nuc10i5fnk					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2269
nuc_10_performance_kit_nuc10i5fnkp					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2270
nuc_10_performance_kit_nuc10i5fnkpa					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2271
nuc_10_performance_kit_nuc10i7fnh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an	https://www.intel.com/content/ww	H-INT-NUC_-071221/2272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w/us/en/security-center/advisory/intel-sa-00567.html	
nuc_10_performance_kit_nuc10i7fnhaa					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2273
nuc_10_performance_kit_nuc10i7fnhc					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2274
nuc_10_performance_kit_nuc10i7fnhja					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2275
nuc_10_performance_kit_nuc10i7fnk					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-	H-INT-NUC_-071221/2276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2021-33086**	center/advisory/intel-sa-00567.html	
nuc_10_performance_kit_nuc10i7fnkp					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2277
nuc_10_performance_kit_nuc10i7fnkpa					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2278
nuc_11_compute_element_cm11ebc4w					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2279
nuc_11_compute_element_cm11ebi38w					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-NUC_-071221/2280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00567.html	
nuc_11_compute_element_cm11ebi58w					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2281
nuc_11_compute_element_cm11ebi716w					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2282
nuc_11_enthusiast_kit_nuc11phki7c					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2283
nuc_11_enthusiast_mini_pc_nuc11phki7caa					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2284
nuc_11_performance_kit_nuc11pahi3					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2285
nuc_11_performance_kit_nuc11pahi5					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2286
nuc_11_performance_kit_nuc11pahi7					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2287
nuc_11_performance_kit_nuc11paki3					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2288
nuc_11_performance_kit_nuc11paki5					
Out-of-bounds	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R)	https://www.intel.com/	H-INT-NUC_-071221/2289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	content/www/us/en/security-center/advisory/intel-sa-00567.html	
nuc_11_performance_kit_nuc11paki7					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2290
nuc_11_performance_mini_pc_nuc11paqi50wa					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2291
nuc_11_performance_mini_pc_nuc11paqi70qa					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2292
nuc_11_pro_board_nuc11tnbi3					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to	https://www.intel.com/content/www/us/en/se	H-INT-NUC_-071221/2293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	curity-center/advisory/intel-sa-00567.html	
nuc_11_pro_board_nuc11tnbi5					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2294
nuc_11_pro_board_nuc11tnbi7					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2295
nuc_11_pro_kit_nuc11tnhi3					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2296
nuc_11_pro_kit_nuc11tnhi30l					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-NUC_-071221/2297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-33086	ory/intel-sa-00567.html	
nuc_11_pro_kit_nuc11tnhi30p					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2298
nuc_11_pro_kit_nuc11tnhi5					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2299
nuc_11_pro_kit_nuc11tnhi50l					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2300
nuc_11_pro_kit_nuc11tnhi50w					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nuc_11_pro_kit_nuc11tnhi7					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2302
nuc_11_pro_kit_nuc11tnhi70l					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2303
nuc_11_pro_kit_nuc11tnhi70q					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2304
nuc_11_pro_kit_nuc11tnki3					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2305
nuc_11_pro_kit_nuc11tnki5					
Out-of-	17-Nov-21	4.9	Out-of-bounds write in	https://ww	H-INT-NUC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	071221/2306
nuc_11_pro_kit_nuc11tnki7					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2307
nuc_7_business_nuc7i3dnhnc					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2308
nuc_7_business_nuc7i3dnktc					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2309
nuc_7_business_nuc7i5dnbe					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an	https://www.intel.com/content/www	H-INT-NUC_-071221/2310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w/us/en/security-center/advisory/intel-sa-00567.html	
nuc_7_business_nuc7i5dnhe					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2311
nuc_7_business_nuc7i5dnke					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2312
nuc_7_business_nuc7i5dnkpc					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2313
nuc_7_essential_nuc7cjysal					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-	H-INT-NUC_-071221/2314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2021-33086**	center/advisory/intel-sa-00567.html	
nuc_8_business_nuc8i7hnkqc					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2315
nuc_8_compute_element_cm8ccb					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2316
nuc_8_compute_element_cm8i3cb					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2317
nuc_8_compute_element_cm8i5cb					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-NUC_-071221/2318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00567.html	
nuc_8_compute_element_cm8i7cb					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2319
nuc_8_compute_element_cm8pcb					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2320
nuc_8_enthusiast_nuc8i7behga					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2321
nuc_8_enthusiast_nuc8i7bekqa					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2322
nuc_8_enthusiast_nuc8i7hvkva					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2323
nuc_8_enthusiast_nuc8i7hvkvaw					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2324
nuc_8_home_nuc8i3behfa					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2325
nuc_8_home_nuc8i3cysm					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2326
nuc_8_home_nuc8i3cysn					
Out-of-bounds	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R)	https://www.intel.com/	H-INT-NUC_-071221/2327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	content/www/us/en/security-center/advisory/intel-sa-00567.html	
nuc_8_home_nuc8i5behfa					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2328
nuc_8_home_nuc8i5bekpa					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2329
nuc_8_mainstream-g_kit_nuc8i5inh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2330
nuc_8_mainstream-g_kit_nuc8i7inh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to	https://www.intel.com/content/www/us/en/se	H-INT-NUC_-071221/2331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	curity-center/advisory/intel-sa-00567.html	
nuc_8_mainstream-g_mini_pc_nuc8i5inh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2332
nuc_8_mainstream-g_mini_pc_nuc8i7inh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2333
nuc_8_pro_board_nuc8i3pnb					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2334
nuc_8_pro_kit_nuc8i3pnh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-NUC_-071221/2335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-33086	ory/intel-sa-00567.html	
nuc_8_pro_kit_nuc8i3pnk					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2336
nuc_8_rugged_kit_nuc8cchkr					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2337
nuc_9_pro_compute_element_nuc9v7qnb					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2338
nuc_9_pro_compute_element_nuc9vxqnb					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nuc_9_pro_kit_nuc9v7qnx					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2340
nuc_9_pro_kit_nuc9vxqnx					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2341
nuc_board_nuc7i3dnbe					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2342
nuc_board_nuc8cchb					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2343
nuc_kit_nuc6cayh					
Out-of-	17-Nov-21	4.9	Out-of-bounds write in	https://ww	H-INT-NUC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	071221/2344
nuc_kit_nuc6cays					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2345
nuc_kit_nuc7cjyh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2346
nuc_kit_nuc7i3dnhe					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2347
nuc_kit_nuc7i3dnke					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an	https://www.intel.com/content/www	H-INT-NUC_-071221/2348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w/us/en/security-center/advisory/intel-sa-00567.html	
nuc_kit_nuc7pjyh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2349
nuc_kit_nuc8i3be					
Improper Privilege Management	17-Nov-21	4.6	Improper access control in the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC8i3BE, NUC8i5BE, NUC8i7BE before version 1.78.4.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33089**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	H-INT-NUC_-071221/2350
nuc_kit_nuc8i3beh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2351
nuc_kit_nuc8i3behs					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an	https://www.intel.com/content/ww	H-INT-NUC_-071221/2352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w/us/en/security-center/advisory/intel-sa-00567.html	
nuc_kit_nuc8i3bek					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2353
nuc_kit_nuc8i5be					
Improper Privilege Management	17-Nov-21	4.6	Improper access control in the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC8i3BE, NUC8i5BE, NUC8i7BE before version 1.78.4.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33089**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	H-INT-NUC_-071221/2354
nuc_kit_nuc8i5beh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2355
nuc_kit_nuc8i5behs					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an	https://www.intel.com/content/ww	H-INT-NUC_-071221/2356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w/us/en/security-center/advisory/intel-sa-00567.html	
nuc_kit_nuc8i5bek					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2357
nuc_kit_nuc8i7be					
Improper Privilege Management	17-Nov-21	4.6	Improper access control in the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC8i3BE, NUC8i5BE, NUC8i7BE before version 1.78.4.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33089**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	H-INT-NUC_-071221/2358
nuc_kit_nuc8i7beh					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2359
nuc_kit_nuc8i7bek					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an	https://www.intel.com/content/ww	H-INT-NUC_-071221/2360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w/us/en/security-center/advisory/intel-sa-00567.html	
nuc_kit_nuc8i7hnk					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2361
nuc_kit_nuc8i7hvk					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2362
nuc_m15_laptop_kit_lapbc510					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2363
Improper Authentication	17-Nov-21	4.9	Improper authentication in the installer for the Intel(R) NUC M15 Laptop Kit Management Engine driver pack before version 15.0.10.1508 may allow an authenticated user to	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-NUC_-071221/2364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via local access. **CVE ID : CVE-2021-33087**	00569.html	
Incorrect Default Permissions	17-Nov-21	7.2	Incorrect default permissions in the installer for the Intel(R) NUC M15 Laptop Kit Integrated Sensor Hub driver pack before version 5.4.1.4449 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33088**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	H-INT-NUC_-071221/2365
Incorrect Permission Assignment for Critical Resource	17-Nov-21	7.2	Insecure inherited permissions in the installer for the Intel(R) NUC M15 Laptop Kit audio driver pack before version 1.3 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33091**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	H-INT-NUC_-071221/2366
Incorrect Default Permissions	17-Nov-21	7.2	Incorrect default permissions in the installer for the Intel(R) NUC M15 Laptop Kit HID Event Filter driver pack before version 2.2.1.383 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33092**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	H-INT-NUC_-071221/2367
Incorrect Permission Assignment for Critical Resource	17-Nov-21	7.2	Insecure inherited permissions in the installer for the Intel(R) NUC M15 Laptop Kit Serial IO driver pack before version 30.100.2104.1 may allow an authenticated user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-NUC_-071221/2368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2021-33093**	00569.html	
Incorrect Permission Assignment for Critical Resource	17-Nov-21	7.2	Insecure inherited permissions in the installer for the Intel(R) NUC M15 Laptop Kit Keyboard LED Service driver pack before version 1.0.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33094**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	H-INT-NUC_-071221/2369
Unquoted Search Path or Element	17-Nov-21	7.2	Unquoted search path in the installer for the Intel(R) NUC M15 Laptop Kit Keyboard LED Service driver pack before version 1.0.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33095**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	H-INT-NUC_-071221/2370
nuc_m15_laptop_kit_lapbc710					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	H-INT-NUC_-071221/2371
Improper Authentication	17-Nov-21	4.9	Improper authentication in the installer for the Intel(R) NUC M15 Laptop Kit Management Engine driver pack before version 15.0.10.1508 may allow an authenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	H-INT-NUC_-071221/2372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2021-33087**		
Incorrect Default Permissions	17-Nov-21	7.2	Incorrect default permissions in the installer for the Intel(R) NUC M15 Laptop Kit Integrated Sensor Hub driver pack before version 5.4.1.4449 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33088**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	H-INT-NUC_-071221/2373
Incorrect Permission Assignment for Critical Resource	17-Nov-21	7.2	Insecure inherited permissions in the installer for the Intel(R) NUC M15 Laptop Kit audio driver pack before version 1.3 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33091**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	H-INT-NUC_-071221/2374
Incorrect Default Permissions	17-Nov-21	7.2	Incorrect default permissions in the installer for the Intel(R) NUC M15 Laptop Kit HID Event Filter driver pack before version 2.2.1.383 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33092**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	H-INT-NUC_-071221/2375
Incorrect Permission Assignment for Critical Resource	17-Nov-21	7.2	Insecure inherited permissions in the installer for the Intel(R) NUC M15 Laptop Kit Serial IO driver pack before version 30.100.2104.1 may allow an authenticated user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	H-INT-NUC_-071221/2376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2021-33093**		
Incorrect Permission Assignment for Critical Resource	17-Nov-21	7.2	Insecure inherited permissions in the installer for the Intel(R) NUC M15 Laptop Kit Keyboard LED Service driver pack before version 1.0.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33094**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	H-INT-NUC_-071221/2377
Unquoted Search Path or Element	17-Nov-21	7.2	Unquoted search path in the installer for the Intel(R) NUC M15 Laptop Kit Keyboard LED Service driver pack before version 1.0.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33095**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	H-INT-NUC_-071221/2378
pentium_j2850					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2379
pentium_j2900					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-PENT-071221/2380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via physical access. **CVE ID : CVE-2021-0146**	ory/intel-sa-00528.html	
pentium_j3710					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2381
pentium_j4205					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2382
pentium_j6426					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2383
pentium_n3510					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors	https://www.intel.com/content/ww	H-INT-PENT-071221/2384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	w/us/en/security-center/advisory/intel-sa-00528.html	
pentium_n3520					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2385
pentium_n3530					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2386
pentium_n3540					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2387
pentium_n3700					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2388
pentium_n3710					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2389
pentium_n4200					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2390
pentium_n4200e					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0146		
pentium_n6415					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2392
pentium_silver_j5005					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2393
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-PENT-071221/2394
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-PENT-071221/2395
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	H-INT-PENT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	071221/2396
pentium_silver_j5040					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2397
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-PENT-071221/2398
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-PENT-071221/2399
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to	https://www.intel.com/content/www/us/en/security-	H-INT-PENT-071221/2400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	center/advisory/intel-sa-00548.html	
pentium_silver_n5000					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2401
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-PENT-071221/2402
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-PENT-071221/2403
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-PENT-071221/2404
pentium_silver_n5030					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2405
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-PENT-071221/2406
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-PENT-071221/2407
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-PENT-071221/2408
pentium_silver_n6000					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an	https://www.intel.com/content/www/us/en/se	H-INT-PENT-071221/2409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	curity-center/advisory/intel-sa-00528.html	
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-PENT-071221/2410
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-PENT-071221/2411
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-PENT-071221/2412
pentium_silver_n6005					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	H-INT-PENT-071221/2413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0146		
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-PENT-071221/2414
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-PENT-071221/2415
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-PENT-071221/2416
ssd_d-s4510					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2417
ssd_d5-p4320					
Insertion of Sensitive Information	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a	https://www.intel.com/content/ww	H-INT-SSD_-071221/2418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
into Log File			privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	w/us/en/security-center/advisory/intel-sa-00535.html	
ssd_d5-p4326					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2419
ssd_d5-p4420					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2420
ssd_d7-p5500					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2421
ssd_d7-p5600					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure	https://www.intel.com/content/www/us/en/security-	H-INT-SSD_-071221/2422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0148**	center/advisory/intel-sa-00535.html	
ssd_d7-p5608					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2423
ssd_dc_d4512					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2424
ssd_dc_p4500					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2425
ssd_dc_p4501					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-SSD_-071221/2426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00535.html	
ssd_dc_p4510_edsff					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2427
ssd_dc_p4510_u.2					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2428
ssd_dc_p4511_edsff					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2429
ssd_dc_p4511_m.2					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2430
ssd_dc_p4600					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2431
ssd_dc_p4608					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2432
ssd_dc_p4610_u.2					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2433
ssd_dc_p4618					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	H-INT-SSD_-071221/2434
xeon_e-2124					
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-XEON-071221/2435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2436
xeon_e-2124g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2437
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2438
xeon_e-2126g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-XEON-071221/2439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2440
xeon_e-2134					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2441
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2442
xeon_e-2136					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2443
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-XEON-071221/2444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
xeon_e-2144g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2445
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2446
xeon_e-2146g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2447
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-XEON-071221/2448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
xeon_e-2174g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2449
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2450
xeon_e-2176g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2451
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2452
xeon_e-2176m					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2453
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2454
xeon_e-2186g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2455
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2456
xeon_e-2186m					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2458
xeon_e-2224					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2459
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2460
xeon_e-2224g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2462
xeon_e-2226g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2463
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2464
xeon_e-2226ge					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2465
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
xeon_e-2234					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2467
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2468
xeon_e-2236					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2469
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xeon_e-2244g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2471
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2472
xeon_e-2246g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2473
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2474
xeon_e-2254me					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-XEON-071221/2475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2476
xeon_e-2254ml					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2477
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2478
xeon_e-2274g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2480
xeon_e-2276g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2481
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2482
xeon_e-2276m					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2483
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-XEON-071221/2484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
xeon_e-2276me					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2485
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2486
xeon_e-2276ml					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2487
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00562.html	
xeon_e-2278g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2489
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2490
xeon_e-2278ge					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2491
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2492
xeon_e-2278gel					
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	071221/2493
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2494
xeon_e-2286g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2495
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2496
xeon_e-2286m					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-XEON-071221/2497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2498
xeon_e-2288g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2499
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2500
xeon_e-2314					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2501
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-XEON-071221/2502

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
xeon_e-2324g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2503
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2504
xeon_e-2334					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2505
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-XEON-071221/2506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
xeon_e-2336					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2507
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2508
xeon_e-2356g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2509
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2510
xeon_e-2374g					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2511
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2512
xeon_e-2378					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2513
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2514
xeon_e-2378g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2516
xeon_e-2386g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2517
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2518
xeon_e-2388g					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2520
xeon_e3-1220_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2521
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2522
xeon_e3-1225_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2523
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
xeon_e3-1230_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2525
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2526
xeon_e3-1240_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2527
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xeon_e3-1245_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2529
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2530
xeon_e3-1270_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2531
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2532
xeon_e3-1275_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-XEON-071221/2533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2534
xeon_e3-1280_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2535
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2536
xeon_e3-1285_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2538
xeon_e3-1501l_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2539
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2540
xeon_e3-1501m_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2541
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-XEON-071221/2542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
xeon_e3-1505l_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2543
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2544
xeon_e3-1505m_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2545
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00562.html	
xeon_e3-1535m_v6					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2547
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2548
xeon_gold_5315y					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2549
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2550
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for	https://www.intel.com/content/ww	H-INT-XEON-071221/2551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w/us/en/security-center/advisory/intel-sa-00548.html	
xeon_gold_5317					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2552
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2553
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2554
xeon_gold_5318h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2556
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2557
xeon_gold_5318n					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2558
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2559
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	curity-center/advisory/intel-sa-00548.html	
xeon_gold_5318s					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2561
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2562
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2563
xeon_gold_5318y					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2565
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2566
xeon_gold_5320					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2567
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2568
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-XEON-071221/2569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	ory/intel-sa-00548.html	
xeon_gold_5320h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2570
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2571
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2572
xeon_gold_5320t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2573
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	071221/2574
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2575
xeon_gold_6312u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2576
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2577
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0186	00548.html	
xeon_gold_6314u					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2579
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2580
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2581
xeon_gold_6326					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2582
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-XEON-071221/2583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2584
xeon_gold_6328h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2585
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2586
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xeon_gold_6328hl					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2588
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2589
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2590
xeon_gold_6330					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2591
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2593
xeon_gold_6330h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2594
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2595
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2596
xeon_gold_6330n					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2597
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2598
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2599
xeon_gold_6334					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2600
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-	H-INT-XEON-071221/2601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2021-0158**	center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2602
xeon_gold_6336y					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2603
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2604
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2605
xeon_gold_6338					
Improper	17-Nov-21	4.6	Insufficient control flow	https://ww	H-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	071221/2606
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2607
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2608
xeon_gold_6338n					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2609
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-XEON-071221/2610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2611
xeon_gold_6338t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2612
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2613
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2614
xeon_gold_6342					
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-XEON-071221/2615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2616
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2617
xeon_gold_6346					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2618
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2620
xeon_gold_6348					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2621
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2622
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2623
xeon_gold_6348h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-XEON-071221/2624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2625
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2626
xeon_gold_6354					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2627
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2629
xeon_platinum_8351n					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2630
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2631
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2632
xeon_platinum_8352m					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2634
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2635
xeon_platinum_8352s					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2636
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2637
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	H-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	071221/2638
xeon_platinum_8352v					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2639
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2640
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2641
xeon_platinum_8352y					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially	https://www.intel.com/content/www/us/en/security-	H-INT-XEON-071221/2642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2643
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2644
xeon_platinum_8353h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2645
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2646
Improper Input	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK	https://www.intel.com/	H-INT-XEON-071221/2647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	content/www/us/en/security-center/advisory/intel-sa-00548.html	
xeon_platinum_8354h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2648
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2649
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2650
xeon_platinum_8356h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-XEON-071221/2651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2652
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2653
xeon_platinum_8358					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2654
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2655
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for	https://www.intel.com/content/ww	H-INT-XEON-071221/2656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w/us/en/security-center/advisory/intel-sa-00548.html	
xeon_platinum_8358p					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2657
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2658
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2659
xeon_platinum_8360h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2661
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2662
xeon_platinum_8360hl					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2663
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2664
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	curity-center/advisory/intel-sa-00548.html	
xeon_platinum_8360y					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2666
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2667
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2668
xeon_platinum_8362					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2670
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2671
xeon_platinum_8368					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2672
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2673
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-XEON-071221/2674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	ory/intel-sa-00548.html	
xeon_platinum_8368q					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2675
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2676
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2677
xeon_platinum_8376h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2678
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	071221/2679
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2680
xeon_platinum_8376hl					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2681
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2682
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0186	00548.html	
xeon_platinum_8380					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2684
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2685
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2686
xeon_platinum_8380h					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2687
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-XEON-071221/2688

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2689
xeon_platinum_8380hl					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2690
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2691
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xeon_silver_4309y					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2693
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2694
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2695
xeon_silver_4310					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2696
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2698
xeon_silver_4310t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2699
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2700
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2701
xeon_silver_4314					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2702
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2703
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2704
xeon_silver_4316					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2705
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-	H-INT-XEON-071221/2706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2021-0158**	center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	H-INT-XEON-071221/2707
xeon_w-10855m					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2708
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2709
xeon_w-10885m					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2710
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	H-INT-XEON-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	071221/2711
xeon_w-11155mle					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2712
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2713
xeon_w-11155mre					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2714
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-	H-INT-XEON-071221/2715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2021-0158**	center/advisory/intel-sa-00562.html	
xeon_w-11555mle					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2716
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2717
xeon_w-11555mre					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2718
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2719
xeon_w-11855m					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2720
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2721
xeon_w-11865mle					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2722
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2723
xeon_w-11865mre					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2725
xeon_w-11955m					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2726
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2727
xeon_w-1250					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2729
xeon_w-1250e					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2730
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2731
xeon_w-1250p					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2732
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
xeon_w-1250te					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2734
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2735
xeon_w-1270					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2736
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xeon_w-1270e					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2738
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2739
xeon_w-1270p					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2740
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2741
xeon_w-1270te					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-XEON-071221/2742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2743
xeon_w-1290					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2744
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2745
xeon_w-1290e					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2747
xeon_w-1290p					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2748
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2749
xeon_w-1290t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2750
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-XEON-071221/2751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
xeon_w-1290te					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2752
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2753
xeon_w-1350					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2754
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00562.html	
xeon_w-1350p					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2756
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2757
xeon_w-1370					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2758
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2759
xeon_w-1370p					
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	071221/2760
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2761
xeon_w-1390					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2762
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2763
xeon_w-1390p					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-XEON-071221/2764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2765
xeon_w-1390t					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2766
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2767
xeon_w-2123					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2768
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-XEON-071221/2769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
xeon_w-2125					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2770
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2771
xeon_w-2133					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2772
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-XEON-071221/2773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0158	ory/intel-sa-00562.html	
xeon_w-2135					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2774
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2775
xeon_w-2145					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2776
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2777
xeon_w-2155					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2778
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2779
xeon_w-2175					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2780
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2781
xeon_w-2195					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	curity-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2783
xeon_w-2223					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2784
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2785
xeon_w-2225					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2787
xeon_w-2235					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2788
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2789
xeon_w-2245					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2790
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to	https://www.intel.com/content/www/us/en/se	H-INT-XEON-071221/2791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	curity-center/advisory/intel-sa-00562.html	
xeon_w-2255					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2792
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2793
xeon_w-2265					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2794
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xeon_w-2275					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2796
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2797
xeon_w-2295					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2798
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2799
xeon_w-3175x					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R)	https://www.intel.com/content/ww	H-INT-XEON-071221/2800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	w/us/en/security-center/advisory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2801
xeon_w-3223					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2802
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2803
xeon_w-3225					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0157	00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2805
xeon_w-3235					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2806
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2807
xeon_w-3245					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2808
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow	https://www.intel.com/content/ww	H-INT-XEON-071221/2809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	w/us/en/security-center/advisory/intel-sa-00562.html	
xeon_w-3245m					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2810
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2811
xeon_w-3265					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2812
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	H-INT-XEON-071221/2813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00562.html	
xeon_w-3265m					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2814
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2815
xeon_w-3275					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2816
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2817
xeon_w-3275m					
Improper Privilege	17-Nov-21	4.6	Insufficient control flow management in the BIOS	https://www.intel.com/	H-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	content/www/us/en/security-center/advisory/intel-sa-00562.html	071221/2818
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2819
xeon_w-3323					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2820
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2821
xeon_w-3335					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege	https://www.intel.com/content/www/us/en/security-center/advis	H-INT-XEON-071221/2822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via local access. **CVE ID : CVE-2021-0157**	ory/intel-sa-00562.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2823
xeon_w-3345					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2824
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2825
xeon_w-3365					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2826
Improper Input	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some	https://www.intel.com/	H-INT-XEON-071221/2827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	content/www/us/en/security-center/advisory/intel-sa-00562.html	
xeon_w-3375					
Improper Privilege Management	17-Nov-21	4.6	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0157**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2828
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0158**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html	H-INT-XEON-071221/2829
iptime					
c200					
N/A	22-Nov-21	10	ius_get.cgi in IpTime C200 camera allows remote code execution. A remote attacker may send a crafted parameters to the exposed vulnerable web service interface which invokes the arbitrary shell command. **CVE ID : CVE-2021-26614**	N/A	H-IPT-C200-071221/2830
mediatek					
mt5522					
Out-of-	18-Nov-21	2.1	In asf extractor, there is a	https://corp	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	.mediatek.com/product-security-bulletin/November-2021	MT55-071221/2831
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2832
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2833
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT55-071221/2834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	bulletin/November-2021	
mt5527					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2835
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2836
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2837

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2838
mt5597					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2839
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2841
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2842
mt5598					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05561381. **CVE ID : CVE-2021-0620**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2844
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2845
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mt5599					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2847
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2848
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT55-071221/2849
Integer Overflow or	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT55-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	m/product-security-bulletin/November-2021	071221/2850
mt6580					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT65-071221/2851
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT65-071221/2852
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT65-071221/2853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	bulletin/November-2021	
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT65-071221/2854
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT65-071221/2855
mt6731					
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2856

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**		
mt6732					
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2857
mt6735					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2858
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2860
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2861
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**		
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2863
mt6737					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2864
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2865

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0621		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2866
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2867
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2868
Incorrect Default	18-Nov-21	2.1	In Browser app, there is a possible information	https://corp.mediatek.co	H-MED-MT67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	m/product-security-bulletin/November-2021	071221/2869
mt6739					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2870
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2871
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT67-071221/2872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	bulletin/November-2021	
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2873
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2874
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**		
mt6750					
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2876
mt6750s					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2877
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2879
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2880
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05594988. **CVE ID : CVE-2021-0624**		
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2882
mt6752					
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2883
mt6753					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05561381. **CVE ID : CVE-2021-0620**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2885
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2886
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2888
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2889
mt6755					
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2890
mt6755s					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2891
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2892
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2893
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow.	https://corp.mediatek.com/product-	H-MED-MT67-071221/2894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	security-bulletin/November-2021	
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2895
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2896
mt6757					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT67-071221/2897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	ember-2021	
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2898
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2899
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**		
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2901
mt6757c					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2902
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05561383. **CVE ID : CVE-2021-0621**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2904
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2905
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2907
mt6757cd					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2908
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2909
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT67-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	m/product-security-bulletin/November-2021	071221/2910
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2911
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2912
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT67-071221/2913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	ember-2021	
mt6757ch					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2914
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2915
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2917
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2918
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05969704. **CVE ID : CVE-2021-0672**		
mt6758					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2920
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2921
mt6761					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05561395. **CVE ID : CVE-2021-0619**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2923
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2924
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2926
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2927
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2928
mt6762					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	m/product-security-bulletin/November-2021	071221/2929
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2930
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2931
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT67-071221/2932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	ember-2021	
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2933
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2934
mt6763					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2936
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2937
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05561388. **CVE ID : CVE-2021-0622**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2939
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2940
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mt6765					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2942
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2943
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2944
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	m/product-security-bulletin/November-2021	071221/2945
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2946
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2947
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT67-071221/2948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	ember-2021	
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2949
mt6768					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2950
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2952
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2953
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0623		
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2955
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2956
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2957
mt6769					
Out-of-	18-Nov-21	2.1	In ape extractor, there is a	https://corp	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	.mediatek.com/product-security-bulletin/November-2021	MT67-071221/2958
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2959
mt6771					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2960
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow.	https://corp.mediatek.com/product-	H-MED-MT67-071221/2961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	security-bulletin/November-2021	
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2962
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2963
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**		
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2965
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2966
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05969704. **CVE ID : CVE-2021-0672**		
mt6779					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2968
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2969
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0621		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2971
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2972
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2973
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a	https://corp.mediatek.co	H-MED-MT67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	m/product-security-bulletin/November-2021	071221/2974
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2975
mt6781					
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2976
mt6785					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-	H-MED-MT67-071221/2977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	security-bulletin/November-2021	
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2978
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2979
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2981
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2982
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05827158. **CVE ID : CVE-2021-0664**		
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2984
mt6795					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2985
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0672		
mt6797					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2987
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2988
mt6799					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0619		
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT67-071221/2990
mt6833					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/2991
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/2992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/2993
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/2994
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/2995
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow.	https://corp.mediatek.com/product-	H-MED-MT68-071221/2996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	security-bulletin/November-2021	
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/2997
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/2998
mt6853					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/2999

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3000
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3001
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3003
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3004
Use After Free	18-Nov-21	4.6	In edma driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05709376; Issue ID: ALPS05709376. **CVE ID : CVE-2021-0656**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3006
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3007
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3008
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3009

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**		
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273. **CVE ID : CVE-2021-0671**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3010
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3011
mt6853t					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05561395. **CVE ID : CVE-2021-0619**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3013
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3014
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3016
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3017
Use After Free	18-Nov-21	4.6	In edma driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05709376; Issue ID: ALPS05709376. **CVE ID : CVE-2021-0656**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3018
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT68-071221/3019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**	bulletin/November-2021	
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3020
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3021
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0671		
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3023
mt6873					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3024
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3026
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3027
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3028
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow.	https://corp.mediatek.com/product-	H-MED-MT68-071221/3029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	security-bulletin/November-2021	
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3030
Improper Privilege Management	18-Nov-21	4.6	In mdlactl driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05673424; Issue ID: ALPS05673424. **CVE ID : CVE-2021-0655**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3031
Use After Free	18-Nov-21	4.6	In edma driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05709376; Issue ID: ALPS05709376. **CVE ID : CVE-2021-0656**		
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103. **CVE ID : CVE-2021-0657**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3033
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107. **CVE ID : CVE-2021-0658**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3034
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3035
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT68-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	security-bulletin/November-2021	071221/3036
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3037
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3038
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05670581. **CVE ID : CVE-2021-0667**		
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3040
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3041
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3042
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT68-071221/3043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273. **CVE ID : CVE-2021-0671**	bulletin/November-2021	
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3044
mt6875					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3045
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**		
Improper Privilege Management	18-Nov-21	4.6	In mdlactl driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05673424; Issue ID: ALPS05673424. **CVE ID : CVE-2021-0655**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3047
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103. **CVE ID : CVE-2021-0657**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3048
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107. **CVE ID : CVE-2021-0658**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3049
Out-of-	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an	https://corp.mediatek.co	H-MED-MT68-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**	m/product-security-bulletin/November-2021	071221/3050
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3051
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3052
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**		
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3054
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3055
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3056
Out-of-bounds	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This	https://corp.mediatek.com/product-	H-MED-MT68-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273. **CVE ID : CVE-2021-0671**	security-bulletin/November-2021	071221/3057
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3058
mt6877					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3059
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3060

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3061
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3062
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**		
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3064
Use After Free	18-Nov-21	4.6	In edma driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05709376; Issue ID: ALPS05709376. **CVE ID : CVE-2021-0656**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3065
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103. **CVE ID : CVE-2021-0657**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3066
Out-of-bounds	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a	https://corp.mediatek.co	H-MED-MT68-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107. **CVE ID : CVE-2021-0658**	m/product-security-bulletin/November-2021	071221/3067
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3068
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3069
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**		
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3071
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3072
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3073
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT68-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	security-bulletin/November-2021	071221/3074
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3075
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273. **CVE ID : CVE-2021-0671**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3076
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**		
mt6883					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3078
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3079
Improper Privilege Management	18-Nov-21	4.6	In mdlactl driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05673424; Issue ID: ALPS05673424. **CVE ID : CVE-2021-0655**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	18-Nov-21	4.6	In edma driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05709376; Issue ID: ALPS05709376. **CVE ID : CVE-2021-0656**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3081
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103. **CVE ID : CVE-2021-0657**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3082
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107. **CVE ID : CVE-2021-0658**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3083
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**		
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3085
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3086
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3088
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3089
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3090
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273. **CVE ID : CVE-2021-0671**		
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3092
mt6885					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3093
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3095
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3096
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3097

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3098
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3099
Improper Privilege Management	18-Nov-21	4.6	In mdlactl driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05673424; Issue ID: ALPS05673424. **CVE ID : CVE-2021-0655**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3100
Use After Free	18-Nov-21	4.6	In edma driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT68-071221/3101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05709376; Issue ID: ALPS05709376. **CVE ID : CVE-2021-0656**	ember-2021	
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103. **CVE ID : CVE-2021-0657**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3102
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107. **CVE ID : CVE-2021-0658**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3103
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3104

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3105
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3106
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3107
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**		
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3109
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3110
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273. **CVE ID : CVE-2021-0671**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3112
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3113
mt6889					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3114
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow.	https://corp.mediatek.com/product-	H-MED-MT68-071221/3115

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	security-bulletin/November-2021	
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3116
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3117
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**		
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3119
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3120
Improper Privilege Management	18-Nov-21	4.6	In mdlactl driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05673424; Issue ID: ALPS05673424.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0655		
Use After Free	18-Nov-21	4.6	In edma driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05709376; Issue ID: ALPS05709376. **CVE ID : CVE-2021-0656**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3122
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103. **CVE ID : CVE-2021-0657**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3123
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107. **CVE ID : CVE-2021-0658**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3124
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT68-071221/3125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**	ember-2021	
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3126
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3127
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3128

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3129
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3130
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3131
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**		
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273. **CVE ID : CVE-2021-0671**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3133
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3134
mt6891					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05561395. **CVE ID : CVE-2021-0619**		
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3136
Improper Privilege Management	18-Nov-21	4.6	In mdlactl driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05673424; Issue ID: ALPS05673424. **CVE ID : CVE-2021-0655**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3137
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103. **CVE ID : CVE-2021-0657**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3138
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT68-071221/3139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107. **CVE ID : CVE-2021-0658**	bulletin/November-2021	
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3140
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3141
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0666		
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3143
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3144
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3145
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT68-071221/3146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**	ember-2021	
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273. **CVE ID : CVE-2021-0671**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3147
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3148
mt6893					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3150
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3151
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3152

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3153
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3154
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3155
Improper Privilege Management	18-Nov-21	4.6	In mdlactl driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT68-071221/3156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05673424; Issue ID: ALPS05673424. **CVE ID : CVE-2021-0655**	bulletin/November-2021	
Use After Free	18-Nov-21	4.6	In edma driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05709376; Issue ID: ALPS05709376. **CVE ID : CVE-2021-0656**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3157
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103. **CVE ID : CVE-2021-0657**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3158
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0658		
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3160
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3161
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3162
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT68-071221/3163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	ember-2021	
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3164
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3165
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273. **CVE ID : CVE-2021-0671**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3166

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT68-071221/3167
mt8163					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3168
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3169
Integer Overflow or	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	m/product-security-bulletin/November-2021	071221/3170
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3171
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3172
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT81-071221/3173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	ember-2021	
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3174
mt8167					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3175
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3177
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3178
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05585817. **CVE ID : CVE-2021-0623**		
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3180
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3181
mt8167s					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0619		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3183
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3184
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3185
Integer Overflow or	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	m/product-security-bulletin/November-2021	071221/3186
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3187
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3188
mt8168					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT81-071221/3189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	bulletin/November-2021	
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3190
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3191
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3193
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3194
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05969704. **CVE ID : CVE-2021-0672**		
mt8173					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3196
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3197
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0621		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3199
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3200
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3201
Incorrect Default	18-Nov-21	2.1	In Browser app, there is a possible information	https://corp.mediatek.co	H-MED-MT81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	m/product-security-bulletin/November-2021	071221/3202
mt8175					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3203
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3204
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT81-071221/3205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	bulletin/November-2021	
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3206
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3207
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**		
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3209
mt8183					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3210
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3212
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3213
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3214

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3215
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3216
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3217
mt8184					
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow.	https://corp.mediatek.com/product-	H-MED-MT81-071221/3218

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	security-bulletin/November-2021	
mt8185					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3219
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3220
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT81-071221/3221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	ember-2021	
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3222
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3223
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**		
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3225
mt8186					
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3226
mt8195					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3228
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3229
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0622		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3231
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3232
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3233
Use After Free	18-Nov-21	4.6	In edma driver, there is a possible memory corruption due to a use after free. This	https://corp.mediatek.com/product-	H-MED-MT81-071221/3234

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05709376; Issue ID: ALPS05709376. **CVE ID : CVE-2021-0656**	security-bulletin/November-2021	
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103. **CVE ID : CVE-2021-0657**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3235
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107. **CVE ID : CVE-2021-0658**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3236
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559;	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**		
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3238
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3239
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3240
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege	https://corp.mediatek.com/product-security-	H-MED-MT81-071221/3241

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**	bulletin/November-2021	
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273. **CVE ID : CVE-2021-0671**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3242
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT81-071221/3243
mt8321					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3245
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3246
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0622		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3248
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3249
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3250
mt8362a					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3251
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3252
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3253
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow.	https://corp.mediatek.com/product-	H-MED-MT83-071221/3254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	security-bulletin/November-2021	
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3255
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3256
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**		
mt8365					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3258
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3259
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3261
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3262
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0624		
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3264
mt8385					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3265
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3267
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3268
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3269
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow.	https://corp.mediatek.com/product-	H-MED-MT83-071221/3270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	security-bulletin/November-2021	
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3271
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT83-071221/3272
mt8735a					
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3273

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**		
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3274
mt8735b					
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3275
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**		
mt8765					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3277
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3278
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05561383. **CVE ID : CVE-2021-0621**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3280
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3281
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3283
mt8766					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3284
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3285
Integer Overflow or	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT87-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	m/product-security-bulletin/November-2021	071221/3286
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3287
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3288
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT87-071221/3289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	ember-2021	
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3290
mt8768					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3291
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3293
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3294
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05585817. **CVE ID : CVE-2021-0623**		
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3296
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3297
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3298
mt8786					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3299
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3300
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3301
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow.	https://corp.mediatek.com/product-	H-MED-MT87-071221/3302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	security-bulletin/November-2021	
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3303
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3304
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**		
mt8788					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3306
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3307
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3309
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3310
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0624		
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3312
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3313
mt8789					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3314
Out-of-	18-Nov-21	2.1	In asf extractor, there is a	https://corp	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	.mediatek.com/product-security-bulletin/November-2021	MT87-071221/3315
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3316
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3317
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT87-071221/3318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	bulletin/November-2021	
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3319
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3320
mt8791					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3322
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3323
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3325
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3326
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	18-Nov-21	4.6	In edma driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05709376; Issue ID: ALPS05709376. **CVE ID : CVE-2021-0656**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3328
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103. **CVE ID : CVE-2021-0657**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3329
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107. **CVE ID : CVE-2021-0658**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3330
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**		
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3332
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3333
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3335
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273. **CVE ID : CVE-2021-0671**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3336
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3337
mt8797					
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT87-071221/3338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	bulletin/November-2021	
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3339
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3340
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3342
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3343
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0629		
Use After Free	18-Nov-21	4.6	In edma driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05709376; Issue ID: ALPS05709376. **CVE ID : CVE-2021-0656**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3345
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103. **CVE ID : CVE-2021-0657**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3346
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107. **CVE ID : CVE-2021-0658**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3347
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT87-071221/3348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**	ember-2021	
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3349
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3350
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3351

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3352
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID: ALPS05664273. **CVE ID : CVE-2021-0671**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3353
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT87-071221/3354
mt9256					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT92-071221/3355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	bulletin/November-2021	
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3356
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3357
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**		
mt9285					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3359
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3360
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3362
mt9286					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3363
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3364

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0621		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3365
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3366
mt9288					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3368
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3369
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT92-071221/3370
mt9629					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT96-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	m/product-security-bulletin/November-2021	071221/3371
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3372
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3373
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT96-071221/3374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	ember-2021	
mt9631					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3375
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3376
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3378
mt9632					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3379
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3381
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3382
mt9636					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3383

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0620		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3384
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3385
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3386
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption	https://corp.mediatek.co	H-MED-MT96-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	m/product-security-bulletin/November-2021	071221/3387
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3388
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3389
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**		
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3391
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3392
mt9638					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3394
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3395
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3396
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This	https://corp.mediatek.com/product-	H-MED-MT96-071221/3397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	security-bulletin/November-2021	
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3398
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3399
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05670581. **CVE ID : CVE-2021-0667**		
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3401
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3402
mt9639					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3403
Integer	18-Nov-21	2.1	In asf extractor, there is a	https://corp	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	.mediatek.com/product-security-bulletin/November-2021	MT96-071221/3404
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3405
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3406
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT96-071221/3407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	bulletin/November-2021	
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3408
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3409
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0667		
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3411
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3412
mt9650					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3413
Integer Overflow or	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT96-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	m/product-security-bulletin/November-2021	071221/3414
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3415
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3416
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/Nov	H-MED-MT96-071221/3417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	ember-2021	
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3418
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3419
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3420

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3421
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3422
mt9652					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3423
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT96-071221/3424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	bulletin/November-2021	
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3425
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3426
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**		
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3428
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3429
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3430
Improper Handling of	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to	https://corp.mediatek.co	H-MED-MT96-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	m/product-security-bulletin/November-2021	071221/3431
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3432
mt9669					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3433
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3434

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3435
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3436
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05776625. **CVE ID : CVE-2021-0629**		
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3438
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3439
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3440
Improper Handling of Exceptional	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT96-071221/3441

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conditions			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	bulletin/November-2021	
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3442
mt9670					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3443
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3445
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3446
mt9675					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05561381. **CVE ID : CVE-2021-0620**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3448
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3449
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mt9685					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3451
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3452
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3453
Integer Overflow or	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT96-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	m/product-security-bulletin/November-2021	071221/3454
mt9686					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3455
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3456
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT96-071221/3457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	bulletin/November-2021	
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3458
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3459
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**		
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3461
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3462
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3463
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT96-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	security-bulletin/November-2021	071221/3464
mt9688					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3465
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3466
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3467

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT96-071221/3468
mt9931					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3469
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**		
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3471
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3472
mt9950					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05561381. **CVE ID : CVE-2021-0620**		
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3474
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3475
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mt9970					
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3477
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3478
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3479
Integer Overflow or	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT99-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	m/product-security-bulletin/November-2021	071221/3480
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3481
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3482
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**		
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3484
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3485
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3486
mt9980					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3487
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3488
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3489
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow.	https://corp.mediatek.com/product-	H-MED-MT99-071221/3490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	security-bulletin/November-2021	
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3491
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3492
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**		
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3494
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3495
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3496
mt9981					
Out-of-	18-Nov-21	2.1	In asf extractor, there is a	https://corp	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	.mediatek.com/product-security-bulletin/November-2021	MT99-071221/3497
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3498
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3499
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT99-071221/3500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	bulletin/November-2021	
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3501
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3502
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086;	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**		
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3504
Improper Handling of Exceptional Conditions	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3505
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	H-MED-MT99-071221/3506
micron					
ddr4_sdram					
N/A	16-Nov-21	7.9	Modern DRAM devices (PC-	https://com	H-MIC-DDR4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DDR4, LPDDR4X) are affected by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer access patterns, consisting of aggressors with different frequencies, phases, and amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example, this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three major DRAM vendors (Samsung, SK Hynix, Micron) are affected by this vulnerability. For more details, please refer to our	sec.ethz.ch/wp-content/files/blacksmith_sp22.pdf	071221/3507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			publication. **CVE ID : CVE-2021-42114**		
lddr4					
N/A	16-Nov-21	7.9	Modern DRAM devices (PC-DDR4, LPDDR4X) are affected by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer access patterns, consisting of aggressors with different frequencies, phases, and amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example, this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three	https://comsec.ethz.ch/wp-content/files/blacksmith_sp22.pdf	H-MIC-LDDR-071221/3508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			major DRAM vendors (Samsung, SK Hynix, Micron) are affected by this vulnerability. For more details, please refer to our publication. **CVE ID : CVE-2021-42114**		
Mitsubishielectric					
got2000_gt2103-pmbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3509
got2000_gt2103-pmbds					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2103-pmbds2					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3511
got2000_gt2103-pmbls					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all	https://www.mitsubishielectric.co.jp	H-MIT-GOT2-071221/3512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	/psirt/vulnerability/pdf/2021-018.pdf	
got2000_gt2104-rtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3513

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
got2000_gt2107-wtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3514
got2000_gt2308-vtba					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2308-vtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3516
got2000_gt2310-vtba					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2310-vtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3518
got2000_gt2505-vtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2505hs-vtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3520
got2000_gt2506hs-vtbd					
Improper Input	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000	https://www.mitsubishi	H-MIT-GOT2-071221/3521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	electric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	
got2000_gt2507-wtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction.	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20601		
got2000_gt2507-wtsd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3523
got2000_gt2507t-wtsd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2508-vtba					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3525
got2000_gt2508-vtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2508-vtwa					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3527
got2000_gt2508-vtwd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions,	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/	H-MIT-GOT2-071221/3528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	2021-018.pdf	
got2000_gt2510-vtba					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3529
got2000_gt2510-vtbd					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3530
got2000_gt2510-vtwa					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2510-vtwd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3532
got2000_gt2510-wxtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2510-wxtsd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3534
got2000_gt2512-stba					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2512-stbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3536
got2000_gt2512-wxtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all	https://www.mitsubishielectric.co.jp	H-MIT-GOT2-071221/3537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	/psirt/vulnerability/pdf/2021-018.pdf	
got2000_gt2512-wxtsd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3538

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
got2000_gt2705-vtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3539
got2000_gt2708-stba					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2708-stbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3541
got2000_gt2708-vtba					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2708-vtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3543
got2000_gt2710-stba					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2710-stbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3545
got2000_gt2710-vtba					
Improper Input	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000	https://www.mitsubishi	H-MIT-GOT2-071221/3546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	electric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	
got2000_gt2710-vtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction.	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20601		
got2000_gt2710-vtwa					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3548
got2000_gt2710-vtwd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2712-stba					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3550
got2000_gt2712-stbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2712-stwa					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3552
got2000_gt2712-stwd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions,	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/	H-MIT-GOT2-071221/3553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	2021-018.pdf	
got2000_gt2715-xtba					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3554
got2000_gt2715-xtbd					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT2-071221/3555
got_simple_gs2107-wtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT_-071221/3556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got_simple_gs2110-wtbd					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	H-MIT-GOT_-071221/3557
ntt-west					
biz_box_nvr510					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page.	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://ww	H-NTT-BIZ_-071221/3558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20843	w.ntt-west.co.jp/smb/kiki_info/info/211109.html	
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	H-NTT-BIZ_-071221/3559
biz_box_nvr700w					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	H-NTT-BIZ_-071221/3560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	H-NTT-BIZ_-071221/3561
biz_box_rtx1210					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	H-NTT-BIZ_-071221/3562
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier,	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU9116	H-NTT-BIZ_-071221/3563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	1784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	
biz_box_rtx830					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	H-NTT-BIZ_-071221/3564
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/1	H-NTT-BIZ_-071221/3565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	1_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	
Nvidia					
dgx-1_p100					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3566
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3567
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3569
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3570
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3571
dgx-1_v100					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3572

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34399		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3573
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3574
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3575
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-1105**		
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3577
dgx-2					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3578
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3579
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to information disclosure. **CVE ID : CVE-2021-23219**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3581
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3582
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX--071221/3583
dgx_station_a100					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX_-071221/3584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX_-071221/3585
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX_-071221/3586
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX_-071221/3587
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-DGX_-071221/3588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DGX_-071221/3589
drive_constellation					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DRIV-071221/3590
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DRIV-071221/3591
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-DRIV-071221/3592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DRIV-071221/3593
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-DRIV-071221/3594
geforce_gtx_1050					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3595
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra	https://nvid	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	ia.custhelp.com/app/answers/detail/a_id/5263	071221/3596
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3597
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3598
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3599

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3600
geforce_gtx_1050_ti					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3601
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3602
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3604
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3605
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3606
geforce_gtx_1060					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3607

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34399		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3608
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3609
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3610
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-1105**		
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3612
geforce_gtx_1070					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3613
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3614
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to information disclosure. **CVE ID : CVE-2021-23219**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3616
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3617
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3618
geforce_gtx_1070_ti					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3620
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3621
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3622
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-GEFO-071221/3623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3624
geforce_gtx_1080					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3625
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3626
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-GEFO-071221/3627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3628
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3629
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3630
geforce_gtx_1080_ti					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-GEFO-071221/3631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	wers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3632
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3633
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3634
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GEFO-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	om/app/answers/detail/a_id/5263	071221/3635
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3636
geforce_gtx_1650					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3637
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3638
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra	https://nvid	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	ia.custhelp.com/app/answers/detail/a_id/5263	071221/3639
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3640
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3641
geforce_gtx_1650_super					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3642

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34399		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3643
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3644
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3645
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-1105**		
geforce_gtx_1660					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3647
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3648
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3649
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3651
geforce_gtx_1660_super					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3652
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3653
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GEFO-071221/3654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3655
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3656
geforce_gtx_1660_ti					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34399		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3658
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3659
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3660
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-1105**		
geforce_gtx_645					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3662
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3663
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3664
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-GEFO-071221/3665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	wers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3666
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3667
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3668
geforce_gtx_650					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GEFO-071221/3669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3670
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3671
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3672

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3673
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3674
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3675
geforce_gtx_650_ti					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3676

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34399		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3677
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3678
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3679
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3681
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3682
geforce_gtx_650_ti_boost					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3683
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3685
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3686
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3687
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	om/app/answers/detail/a_id/5263	071221/3688
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3689
geforce_gtx_660					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3690
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3691
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra	https://nvid	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	ia.custhelp.com/app/answers/detail/a_id/5263	071221/3692
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3693
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3694
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-1105**		
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3696
geforce_gtx_660_ti					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3697
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3698
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3700
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3701
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3702
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-GEFO-071221/3703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	a_id/5263	
geforce_gtx_670					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3704
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3705
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3706
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra	https://nvid	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	ia.custhelp.com/app/answers/detail/a_id/5263	071221/3707
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3708
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3709
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3710
geforce_gtx_680					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3711
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3712
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3713
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to information disclosure. **CVE ID : CVE-2021-23219**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3715
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3716
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3717
geforce_gtx_690					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3719
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3720
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3721
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-GEFO-071221/3722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3723
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3724
geforce_gtx_745					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3725
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GEFO-071221/3726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3727
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3728
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1088		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3730
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3731
geforce_gtx_750					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3732
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3734
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3735
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3736
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-GEFO-071221/3737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3738
geforce_gtx_750_ti					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3739
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3740
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-GEFO-071221/3741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3742
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3743
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3745
geforce_gtx_760					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3746
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3747
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			availability. **CVE ID : CVE-2021-23217**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3749
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3750
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3751
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. **CVE ID : CVE-2021-1125**		
geforce_gtx_760_ti					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3753
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3754
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3755
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-GEFO-071221/3756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	wers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3757
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3758
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3759
geforce_gtx_770					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GEFO-071221/3760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3761
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3762
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3763

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3764
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3765
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3766
geforce_gtx_780					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3767

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34399		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3768
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3769
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3770
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3772
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3773
geforce_gtx_780_ti					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3774
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3776
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3777
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3778
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	om/app/answers/detail/a_id/5263	071221/3779
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3780
geforce_gtx_950					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3781
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3782
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra	https://nvid	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	ia.custhelp.com/app/answers/detail/a_id/5263	071221/3783
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3784
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3785
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to information disclosure. **CVE ID : CVE-2021-1088**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3787
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3788
geforce_gtx_960					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3789
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3791
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3792
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3793
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-GEFO-071221/3794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	wers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3795
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3796
geforce_gtx_970					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3797
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra	https://nvid	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	ia.custhelp.com/app/answers/detail/a_id/5263	071221/3798
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3799
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3800
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to information disclosure. **CVE ID : CVE-2021-23219**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3802
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3803
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3804
geforce_gtx_980					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3806
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3807
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3808
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	om/app/answers/detail/a_id/5263	071221/3809
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3810
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3811
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3812
geforce_gtx_titan_x					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra	https://nvid	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	ia.custhelp.com/app/answers/detail/a_id/5263	071221/3813
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3814
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3815
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3817
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3818
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3819
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3820

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. **CVE ID : CVE-2021-1125**		
geforce_gt_605					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3821
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3822
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3823
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-GEFO-071221/3824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	wers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3825
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3826
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3827
geforce_gt_610					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GEFO-071221/3828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3829
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3830
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3831

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3832
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3833
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3834
geforce_gt_620					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3835

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34399		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3836
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3837
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3838
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3840
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3841
geforce_gt_625					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3842
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3844
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3845
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3846
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	om/app/answers/detail/a_id/5263	071221/3847
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3848
geforce_gt_630					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3849
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3850
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra	https://nvid	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	ia.custhelp.com/app/answers/detail/a_id/5263	071221/3851
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3852
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3853
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-1105**		
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3855
geforce_gt_635					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3856
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3857
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3859
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3860
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3861
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-GEFO-071221/3862

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	a_id/5263	
geforce_gt_640					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3863
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3864
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3865
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra	https://nvid	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	ia.custhelp.com/app/answers/detail/a_id/5263	071221/3866
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3867
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3868
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3869
geforce_gt_705					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3870
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3871
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3872
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to information disclosure. **CVE ID : CVE-2021-23219**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3874
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3875
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3876
geforce_gt_710					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3878
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3879
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3880
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-GEFO-071221/3881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3882
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3883
geforce_gt_720					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3884
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GEFO-071221/3885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3886
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3887
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1088		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3889
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3890
geforce_gt_730					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3891
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3893
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3894
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3895
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-GEFO-071221/3896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3897
geforce_gt_740					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3898
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3899
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-GEFO-071221/3900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3901
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3902
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3904
geforce_rtx_2060					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3905
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3906
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3908
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3909
geforce_rtx_2060_super					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3910
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3912
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3913
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3914
geforce_rtx_2070					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-GEFO-071221/3915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3916
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3917
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3918
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-GEFO-071221/3919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	wers/detail/a_id/5263	
geforce_rtx_2070_super					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3920
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3921
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3922
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra	https://nvid	H-NVI-GEFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	ia.custhelp.com/app/answers/detail/a_id/5263	071221/3923
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3924
geforce_rtx_2080					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3925
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3927
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3928
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3929
geforce_rtx_2080_super					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3931
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3932
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3933
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-GEFO-071221/3934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
geforce_rtx_2080_ti					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3935
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3936
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3937
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GEFO-071221/3938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GEFO-071221/3939
gtx_titan					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3940
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3941

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34400		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3942
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3943
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3944
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**		
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3946
gtx_titan_black					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3947
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3948
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3950
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3951
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3952
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-GTX_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	om/app/answers/detail/a_id/5263	071221/3953
gtx_titan_z					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3954
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3955
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-23217		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3957
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3958
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3959
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-GTX_-071221/3960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1125		
jetson_agx_xavier_16gb					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-071221/3961
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-071221/3962
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-071221/3963
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-071221/3964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-071221/3965
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-071221/3966
jetson_agx_xavier_32gb					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-071221/3967
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3969
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3970
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3971
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-JETS-081221/3972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	a_id/5263	
jetson_agx_xavier_8gb					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3973
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3974
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3975
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-JETS-081221/3976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3977
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3978
jetson_nano					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3979
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-JETS-081221/3980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3981
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3982
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-23219		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3984
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3985
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3986
jetson_tx1					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3988
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3989
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3990
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-JETS-081221/3991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	wers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3992
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3993
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3994
jetson_tx2					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-JETS-081221/3995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3996
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3997
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/3999
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4000
jetson_tx2i					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4001
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34400		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4003
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4004
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4005
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1125		
jetson_tx2_4gb					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4007
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4008
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4009
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4011
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4012
jetson_tx2_nx					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4013
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4015
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4016
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4017
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-JETS-081221/4018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	a_id/5263	
jetson_xavier_nx					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4019
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4020
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4021
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-JETS-081221/4022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4023
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-JETS-081221/4024
nvidia_hgx-2					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4025
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-NVID-081221/4026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4027
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4028
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4030
nvidia_t1000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4031
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4032
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4034
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4035
nvidia_t2000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4036
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4038
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4039
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4040
nvidia_t4					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-NVID-081221/4041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4042
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4043
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4044
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-NVID-081221/4045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	wers/detail/a_id/5263	
nvidia_t400					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4046
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4047
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4048
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra	https://nvid	H-NVI-NVID-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	ia.custhelp.com/app/answers/detail/a_id/5263	081221/4049
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4050
nvidia_t600					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4051
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4053
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4054
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-NVID-081221/4055
quadro_gv100					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4057
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4058
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4059
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4061
quadro_m1000m					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4062
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4063
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal	https://nvidia.custhelp.com/app/ans	H-NVI-QUAD-081221/4064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	wers/detail/a_id/5263	
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4065
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4066
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1088		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4068
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4069
quadro_m1200					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4070
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4072
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4073
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4074
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4076
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4077
quadro_m2000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4078
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-QUAD-081221/4079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	wers/detail/a_id/5263	
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4080
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4081
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4082

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4083
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4084
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4085
quadro_m2000m					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4086

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34399		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4087
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4088
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4089
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4090

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4091
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4092
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4093
quadro_m2200					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4095
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4096
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4097

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4098
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4099
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4100
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
quadro_m3000m					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4102
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4103
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4104
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4106
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4107
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4108
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	a_id/5263	
quadro_m4000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4110
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4111
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4112
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-QUAD-081221/4113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4114
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4115
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1105		
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4117
quadro_m4000m					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4118
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4119
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4121
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4122
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4123
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4125
quadro_m5000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4126
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4127
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal	https://nvidia.custhelp.com/app/ans	H-NVI-QUAD-081221/4128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	wers/detail/a_id/5263	
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4129
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4130
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1088		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4132
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4133
quadro_m5000m					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4134
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4136
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4137
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4138
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4140
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4141
quadro_m500m					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4142
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-QUAD-081221/4143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	wers/detail/a_id/5263	
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4144
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4145
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4146

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4147
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4148
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4149
quadro_m520					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4150

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34399		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4151
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4152
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4153
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4155
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4156
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4157
quadro_m5500					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4159
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4160
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4161

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4162
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4163
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4164
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
quadro_m6000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4166
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4167
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4168
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4170
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4171
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4172
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	a_id/5263	
quadro_m600m					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4174
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4175
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4176
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-QUAD-081221/4177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4178
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4179
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1105		
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4181
quadro_m620					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4182
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4183
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4185
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4186
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4187
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4189
quadro_p1000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4190
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4191
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-QUAD-081221/4192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	wers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4193
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4194
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4195
quadro_p2000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-QUAD-081221/4196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4197
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4198
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4200
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4201
quadro_p2200					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4202
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34400		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4204
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4205
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4206
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1125		
quadro_p3000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4208
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4209
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4210
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4212
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4213
quadro_p3200					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4214
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4216
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4217
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4218
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	a_id/5263	
quadro_p400					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4220
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4221
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4222
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4224
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4225
quadro_p4000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4226
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-QUAD-081221/4227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4228
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4229
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4231
quadro_p4200					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4232
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4233
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4235
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4236
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4237
quadro_p500					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4238

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34399		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4239
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4240
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4241
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-1105**		
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4243
quadro_p5000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4244
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4245
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to information disclosure. **CVE ID : CVE-2021-23219**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4247
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4248
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4249
quadro_p520					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4251
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4252
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4253
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4255
quadro_p5200					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4256
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4257
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4259
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4260
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4261
quadro_p600					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-QUAD-081221/4262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	wers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4263
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4264
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4265
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-QUAD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	om/app/answers/detail/a_id/5263	081221/4266
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4267
quadro_p6000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4268
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4269
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra	https://nvid	H-NVI-QUAD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	ia.custhelp.com/app/answers/detail/a_id/5263	081221/4270
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4271
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4272
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4273
quadro_p620					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4274
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4275
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4276
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1088		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4278
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4279
quadro_rtx_3000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4280
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4282
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4283
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4284
quadro_rtx_4000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4286
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4287
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4288
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
quadro_rtx_5000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4290
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4291
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4292
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-QUAD-081221/4293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4294
quadro_rtx_6000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4295
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4296

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34400		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4297
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4298
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4299
quadro_rtx_8000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4301
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4302
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4303
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
quadro_t1000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4305
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4306
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4307
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-QUAD-081221/4308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	wers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4309
quadro_t2000					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4310
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34400		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4312
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4313
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4314
quadro_t400					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4316
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4317
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4318
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-QUAD-081221/4319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
quadro_t600					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4320
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4321
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4322
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-QUAD-081221/4323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	wers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-QUAD-081221/4324
shield_tv					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4325
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34400		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4327
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4328
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4329
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4331
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4332
shield_tv_pro					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4333
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-SHIE-081221/4334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	a_id/5263	
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4335
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4336
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4338
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4339
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-SHIE-081221/4340
tesla_m10					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4341

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34399		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4342
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4343
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4344
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4345

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4346
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4347
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4348
tesla_m2050					
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-TESL-081221/4349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	a_id/5263	
tesla_m2070					
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4350
tesla_m2070q					
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4351
tesla_m2090					
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**		
tesla_m4					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4353
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4354
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4355
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra	https://nvid	H-NVI-TESL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	ia.custhelp.com/app/answers/detail/a_id/5263	081221/4356
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4357
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4358
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-1105**		
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4360
tesla_m40					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4361
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4362
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4364
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4365
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4366
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-TESL-081221/4367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	wers/detail/a_id/5263	
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4368
tesla_m6					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4369
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4370
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-TESL-081221/4371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4372
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4373
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure. **CVE ID : CVE-2021-1088**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4375
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4376
tesla_m60					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4377
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4379
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4380
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4381
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-TESL-081221/4382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4383
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4384
tesla_p100					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4385
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-TESL-081221/4386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4387
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4388
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-23219		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4390
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4391
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4392
tesla_p4					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4394
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4395
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4396
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**		
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4398
tesla_p40					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4399
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4400
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4402
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4403
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4404
tesla_p6					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-TESL-081221/4405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4406
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4407
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4408
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-TESL-081221/4409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	wers/detail/a_id/5263	
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4410
tesla_v100					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4411
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4412
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-TESL-081221/4413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	om/app/answers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4414
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4415
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4416
tesla_v100s					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra	https://nvid	H-NVI-TESL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	ia.custhelp.com/app/answers/detail/a_id/5263	081221/4417
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4418
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4419
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4420

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4421
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TESL-081221/4422
titan_rtx					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4423
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34400		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4425
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4426
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4427
titan_v					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**		
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4429
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4430
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4431
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-TITA-081221/4432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	a_id/5263	
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4433
titan_x					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4434
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4435
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may	https://nvidia.custhelp.com/app/answers/detail/	H-NVI-TITA-081221/4436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4437
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4438
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4439
titan_xp					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal	https://nvidia.custhelp.com/app/ans	H-NVI-TITA-081221/4440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	wers/detail/a_id/5263	
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4441
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4442
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4443
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	H-NVI-TITA-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	om/app/answers/detail/a_id/5263	081221/4444
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	H-NVI-TITA-081221/4445
Philips					
mri_1.5t					
Exposure of Resource to Wrong Sphere	19-Nov-21	2.1	Philips MRI 1.5T and MRI 3T Version 5.x.x exposes sensitive information to an actor not explicitly authorized to have access. **CVE ID : CVE-2021-42744**	https://www.usa.philips.com/healthcare/about/customer-support/product-security	H-PHI-MRI_-081221/4446
Incorrect Ownership Assignment	19-Nov-21	2.1	Philips MRI 1.5T and MRI 3T Version 5.x.x assigns an owner who is outside the intended control sphere to a resource. **CVE ID : CVE-2021-26248**	https://www.usa.philips.com/healthcare/about/customer-support/product-security	H-PHI-MRI_-081221/4447
Improper Access Control	19-Nov-21	5	Philips MRI 1.5T and MRI 3T Version 5.x.x does not restrict or incorrectly restricts access to a resource from an	https://www.usa.philips.com/healthcare/about/	H-PHI-MRI_-081221/4448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actor. **CVE ID : CVE-2021-26262**	customer-support/product-security	
mri_3t					
Exposure of Resource to Wrong Sphere	19-Nov-21	2.1	Philips MRI 1.5T and MRI 3T Version 5.x.x exposes sensitive information to an actor not explicitly authorized to have access. **CVE ID : CVE-2021-42744**	https://www.usa.philips.com/healthcare/about/customer-support/product-security	H-PHI-MRI_-081221/4449
Incorrect Ownership Assignment	19-Nov-21	2.1	Philips MRI 1.5T and MRI 3T Version 5.x.x assigns an owner who is outside the intended control sphere to a resource. **CVE ID : CVE-2021-26248**	https://www.usa.philips.com/healthcare/about/customer-support/product-security	H-PHI-MRI_-081221/4450
Improper Access Control	19-Nov-21	5	Philips MRI 1.5T and MRI 3T Version 5.x.x does not restrict or incorrectly restricts access to a resource from an unauthorized actor. **CVE ID : CVE-2021-26262**	https://www.usa.philips.com/healthcare/about/customer-support/product-security	H-PHI-MRI_-081221/4451
Qnap					
nas					
Cross-Site Request Forgery (CSRF)	20-Nov-21	6.8	We have already fixed this vulnerability in the following versions of QmailAgent: QmailAgent 3.0.2 (2021/08/25) and later **CVE ID : CVE-2021-34358**	https://www.qnap.com/en/security-advisory/qsa-21-49	H-QNA-NAS-081221/4452
Improper	20-Nov-21	4.3	A reflected cross-site scripting	https://ww	H-QNA-NAS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			(XSS) vulnerability has been reported to affect QNAP NAS running Ragic Cloud DB. If exploited, this vulnerability allows remote attackers to inject malicious code. QNAP have already disabled and removed Ragic Cloud DB from the QNAP App Center, pending a security patch from Ragic. **CVE ID : CVE-2021-38681**	w.qnap.com/en/security-advisory/qsa-21-48	081221/4453
Samsung					
ddr4_sdram					
N/A	16-Nov-21	7.9	Modern DRAM devices (PC-DDR4, LPDDR4X) are affected by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer access patterns, consisting of aggressors with different frequencies, phases, and amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example,	https://comsec.ethz.ch/wp-content/files/blacksmith_sp22.pdf	H-SAM-DDR4-081221/4454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three major DRAM vendors (Samsung, SK Hynix, Micron) are affected by this vulnerability. For more details, please refer to our publication. **CVE ID : CVE-2021-42114**		
lddr4					
N/A	16-Nov-21	7.9	Modern DRAM devices (PC-DDR4, LPDDR4X) are affected by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer access patterns, consisting of aggressors with different frequencies, phases, and amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This	https://comsec.ethz.ch/wp-content/files/blacksmith_sp22.pdf	H-SAM-LDDR-081221/4455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example, this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three major DRAM vendors (Samsung, SK Hynix, Micron) are affected by this vulnerability. For more details, please refer to our publication. **CVE ID : CVE-2021-42114**		
secomea					
gatemanager_8250					
N/A	22-Nov-21	5	This issue affects: Secomea GateManager All versions prior to 9.6. Improper Check of host header in web server of Secomea GateManager allows attacker to cause browser cache poisoning. **CVE ID : CVE-2021-32004**	https://www.secomea.com/support/cybersecurity-advisory/#4578	H-SEC-GATE-081221/4456
skhynix					
ddr4_sdram					
N/A	16-Nov-21	7.9	Modern DRAM devices (PC-DDR4, LPDDR4X) are affected by a vulnerability in their	https://comsec.ethz.ch/wp-	H-SKH-DDR4-081221/4457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer access patterns, consisting of aggressors with different frequencies, phases, and amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example, this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three major DRAM vendors (Samsung, SK Hynix, Micron) are affected by this vulnerability. For more details, please refer to our publication. **CVE ID : CVE-2021-42114**	content/files/blacksmith_sp22.pdf	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
lddr4					
N/A	16-Nov-21	7.9	Modern DRAM devices (PC-DDR4, LPDDR4X) are affected by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer access patterns, consisting of aggressors with different frequencies, phases, and amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example, this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three major DRAM vendors (Samsung, SK Hynix, Micron) are affected by this	https://comsec.ethz.ch/wp-content/files/blacksmith_sp22.pdf	H-SKH-LDDR-081221/4458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. For more details, please refer to our publication. **CVE ID : CVE-2021-42114**		
Trane					
ascend_air-cooled_chiller_acr					
Improper Control of Generation of Code ('Code Injection')	22-Nov-21	4.6	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software. **CVE ID : CVE-2021-38448**	https://us-cert.cisa.gov/ics/advisories/icsa-21-266-01	H-TRA-ASCE-081221/4459
intellipak_1					
Improper Control of Generation of Code ('Code Injection')	22-Nov-21	4.6	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software. **CVE ID : CVE-2021-38448**	https://us-cert.cisa.gov/ics/advisories/icsa-21-266-01	H-TRA-INTE-081221/4460
intellipak_2					
Improper Control of Generation of Code ('Code Injection')	22-Nov-21	4.6	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software. **CVE ID : CVE-2021-38448**	https://us-cert.cisa.gov/ics/advisories/icsa-21-266-01	H-TRA-INTE-081221/4461
odyssey_split_systems					
Improper Control of Generation of Code	22-Nov-21	4.6	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could	https://us-cert.cisa.gov/ics/advisories/icsa-21-	H-TRA-ODYS-081221/4462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			craft code to alter the intended controller flow of the software. **CVE ID : CVE-2021-38448**	266-01	
Yamaha					
nvr510					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	H-YAM-NVR5-081221/4463
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/21110	H-YAM-NVR5-081221/4464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				9.html	
nvr700w					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	H-YAM-NVR7-081221/4465
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	H-YAM-NVR7-081221/4466
rtx1210					
Inclusion of Functionality	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI	http://www.rtpro.yamah	H-YAM-RTX1-081221/4467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
from Untrusted Control Sphere			of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	a.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	H-YAM-RTX1-081221/4468
rtx830					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://busi	H-YAM-RTX8-081221/4469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	ness.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	H-YAM-RTX8-081221/4470
Operating System					
ABB					
rtu500_firmware					
Improper Input Validation	26-Nov-21	7.1	Improper Input Validation vulnerability in the APDU parser in the Bidirectional Communication Interface (BCI) IEC 60870-5-104 function of Hitachi Energy RTU500 series allows an attacker to cause the receiving RTU500 CMU of	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000063&LanguageCode=en&DocumentPart	O-ABB-RTU5-081221/4471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which the BCI is enabled to reboot when receiving a specially crafted message. By default, BCI IEC 60870-5-104 function is disabled (not configured). This issue affects: Hitachi Energy RTU500 series CMU Firmware version 12.0.* (all versions); CMU Firmware version 12.2.* (all versions); CMU Firmware version 12.4.* (all versions). **CVE ID : CVE-2021-35533**	Id=&Action=Launch	
Amazon					
freertos					
N/A	17-Nov-21	7.2	Amazon FreeRTOS 10.2.0 through 10.4.5 on the ARMv7-M and ARMv8-M MPU platforms does not prevent non-kernel code from calling the xPortRaisePrivilege and vPortResetPrivilege internal functions. This is fixed in 10.4.6 and in 10.4.3-LTS Patch 2. **CVE ID : CVE-2021-43997**	N/A	O-AMA-FREE-081221/4472
AMD					
epyc_7001_firmware					
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4473
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/4474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4475
epyc_7002_firmware					
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4476
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4477
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4479
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4480
epyc_7003_firmware					
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4481
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/4482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				etin/amd-sb-1021	
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4483
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4484
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4485
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4486
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System	https://www.amd.com/	O-AMD-EPYC-081221/4487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	en/corporate/product-security/bulletin/amd-sb-1021	
epyc_7232p_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4488
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4489
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4490
Use of Insufficiently	16-Nov-21	5	Persistent platform private key may not be protected	https://www.amd.com/	O-AMD-EPYC-081221/4491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Random Values			with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	en/corporate/product-security/bulletin/amd-sb-1021	
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4492
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4493
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4494
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4495
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources.	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26330	sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4497
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4498
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4499
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4500
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit	https://www.amd.com/	O-AMD-EPYC-081221/4501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	en/corporate/product-security/bulletin/amd-sb-1021	
epyc_7251_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4502
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4503
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4504
Use of	16-Nov-21	5	Persistent platform private	https://ww	O-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Random Values			key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	081221/4505
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4506
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4507
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4508
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
epyc_7252_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4510
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4511
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4512
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4513
Integer Overflow or	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience	https://www.amd.com/	O-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	en/corporate/product-security/bulletin/amd-sb-1021	081221/4514
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4515
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4516
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4517
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26336		
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4519
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4520
epyc_7261_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4521
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of service of the PSP **CVE ID : CVE-2021-26320**	sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4523
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4524
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4525
epyc_7262_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4527
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4528
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4529
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4530
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4531
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a	https://www.amd.com/	O-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	en/corporate/product-security/bulletin/amd-sb-1021	081221/4532
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4533
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4534
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4535
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4536

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potential lack of system resources. **CVE ID : CVE-2021-26338**	sb-1021	
epyc_7272_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4537
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4538
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4539
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”.	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/4540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26322	etin/amd-sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4541
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4542
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4543
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4544
Improper Restriction of Operations	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4546
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4547
epyc_7281_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4548
Improper Certificate	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK)	https://www.amd.com/	O-AMD-EPYC-081221/4549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	en/corporate/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4550
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4551
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4552
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4553
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4555
epyc_7282_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4556
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4557
Improper Neutralizatio	16-Nov-21	4.9	Insufficient ID command validation in the SEV	https://www.amd.com/	O-AMD-EPYC-081221/4558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	en/corporate/product-security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4559
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4560
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4561
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4562
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	security/bulletin/amd-sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4564
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4565
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4566
epyc_72f3_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects:	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/4567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	etin/amd-sb-1021	
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4568
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4569
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4570
Use of Insufficiently Random	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/4571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Values			potential "two time pad attack". **CVE ID : CVE-2021-26322**	e/product-security/bulletin/amd-sb-1021	
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4572
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4573
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4574
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4575
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4577
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4578
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4579
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4580
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/4581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	etin/amd-sb-1021	
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4582
epyc_7301_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4583
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4584
Improper Neutralization of Special Elements	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4586
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4587
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4588
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4589
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	sb-1021	
epyc_7302p_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4591
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4592
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4593
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack”. **CVE ID : CVE-2021-26322**	security/bulletin/amd-sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4595
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4596
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4597
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4598
Improper Restriction of	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/4599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4600
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4601
epyc_7302_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4602
Improper	16-Nov-21	2.1	Insufficient validation of the	https://ww	O-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Certificate Validation			AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	081221/4603
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4604
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4605
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4606
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4607
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/4608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4609
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4610
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4611
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4612

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26338**	sb-1021	
epyc_7313p_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4613
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4614
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4615
Improper Neutralizatio	16-Nov-21	4.9	Insufficient ID command validation in the SEV	https://www.amd.com/	O-AMD-EPYC-081221/4616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	en/corporate/product-security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4617
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4618
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4619
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4620
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/4621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				etin/amd-sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4622
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4623
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4624
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4625
Improper Restriction of Operations	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4627
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4628
epyc_7313_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4629
Insufficient Verification	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot	https://www.amd.com/	O-AMD-EPYC-081221/4630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Data Authenticity			rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	en/corporate/product-security/bulletin/amd-sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4631
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4632
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4633
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4634

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4635
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4636
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4637
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4638
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4639
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/4640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4641
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4642
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4643
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4644

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26338**	sb-1021	
epyc_7343_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4645
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4646
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4647
Improper Neutralizatio	16-Nov-21	4.9	Insufficient ID command validation in the SEV	https://www.amd.com/	O-AMD-EPYC-081221/4648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	en/corporate/product-security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4649
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4650
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4651
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4652
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/4653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				etin/amd-sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4654
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4655
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4656
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4657
Improper Restriction of Operations	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4659
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4660
epyc_7351p_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4661
Improper Certificate	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK)	https://www.amd.com/	O-AMD-EPYC-081221/4662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	en/corporate/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4663
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4664
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4665
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4666
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4668
epyc_7351_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4669
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4670
Improper Neutralizatio	16-Nov-21	4.9	Insufficient ID command validation in the SEV	https://www.amd.com/	O-AMD-EPYC-081221/4671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	en/corporate/product-security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4672
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4673
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4674
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4675
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	security/bulletin/amd-sb-1021	
epyc_7352_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4677
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4678
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4679
Use of Insufficiently	16-Nov-21	5	Persistent platform private key may not be protected	https://www.amd.com/	O-AMD-EPYC-081221/4680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Random Values			with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	en/corporate/product-security/bulletin/amd-sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4681
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4682
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4683
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4684
Improper	16-Nov-21	4.9	Insufficient bounds checking	https://ww	O-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	081221/4685
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4686
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4687
epyc_7371_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26312		
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4689
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4690
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4691
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4692
epyc_73f3_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	sb-1021	
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4694
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4695
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4696
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4697

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack”. **CVE ID : CVE-2021-26322**	security/bulletin/amd-sb-1021	
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4698
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4699
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4700
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4701
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4703
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4704
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4705
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4706
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/4707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	etin/amd-sb-1021	
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4708
epyc_7401p_firmware					
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4709
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4710
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
epyc_7401_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4712
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4713
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4714
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4715
Integer Overflow or	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience	https://www.amd.com/	O-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	en/corporate/product-security/bulletin/amd-sb-1021	081221/4716
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4717
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4718
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4719
epyc_7402p_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4721
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4722
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4723
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4724
Out-of-bounds	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a	https://www.amd.com/	O-AMD-EPYC-081221/4725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	en/corporate/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4726
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4727
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4728
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4729

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26337		
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4730
epyc_7402_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4731
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4732
Improper Neutralization of Special Elements used in a Command	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP.	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			**CVE ID : CVE-2021-26321**	sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4734
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4735
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4736
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4737
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2021-26335**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4739
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4740
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4741
epyc_7413_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4743
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4744
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4745
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4746

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4747
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4748
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4749
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4750
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4751
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26330**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4753
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4754
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4755
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4757
epyc_7443p_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4758
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4759
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4761
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4762
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4763
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4764
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4766
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4767
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4768
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4769
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2021-26335**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4771
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4772
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4773
epyc_7443_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4775
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4776
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4777
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4778

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4779
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4780
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4781
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4782
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4783
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26330**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4785
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4786
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4787
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4789
epyc_7451_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4790
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4791
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4792

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4793
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4794
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4795
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4796
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4797

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
epyc_7452_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4798
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4799
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4800
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4801
Integer Overflow or	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience	https://www.amd.com/	O-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	en/corporate/product-security/bulletin/amd-sb-1021	081221/4802
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4803
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4804
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4805
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26336		
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4807
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4808
epyc_7453_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4809
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4811
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4812
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4813
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4814
Improper Input	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/4815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	e/product-security/bulletin/amd-sb-1021	
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4816
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4817
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4818
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4819
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26331		
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4821
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4822
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4823
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4824
epyc_74f3_firmware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4825
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4826
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4827
Improper Neutralization of Special Elements used in a Command	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP.	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			**CVE ID : CVE-2021-26321**	sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4829
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4830
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4831
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4832
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4833
Integer Overflow or	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience	https://www.amd.com/	O-AMD-EPYC-081221/4834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	en/corporate/product-security/bulletin/amd-sb-1021	
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4835
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4836
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4837
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26336		
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4839
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4840
epyc_7501_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4841
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of service of the PSP **CVE ID : CVE-2021-26320**	sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4843
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4844
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4845
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4846
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26331		
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4848
epyc_7502p_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4849
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4850
Improper Neutralization of Special Elements used in a	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/4851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			the PSP. **CVE ID : CVE-2021-26321**	etin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4852
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4853
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4854
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4855
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4857
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4858
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4859
epyc_7502_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4861
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4862
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4863
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4864
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/4865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may result in a loss of resources. **CVE ID : CVE-2021-26330**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4866
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4867
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4868
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26337		
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4870
epyc_7513_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4871
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4872
Improper Certificate	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK)	https://www.amd.com/	O-AMD-EPYC-081221/4873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	en/corporate/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4874
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4875
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4876
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4877
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity.	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26326	security/bulletin/amd-sb-1021	
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4879
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4880
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4881
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4882
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4884
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4885
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4886
epyc_7532_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4888
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4889
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4890
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4891
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/4892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may result in a loss of resources. **CVE ID : CVE-2021-26330**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4893
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4894
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4895
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26337		
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4897
epyc_7542_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4898
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4899
Improper Neutralization of Special Elements used in a Command	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP.	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			**CVE ID : CVE-2021-26321**	sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4901
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4902
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4903
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4904
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2021-26335**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4906
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4907
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4908
epyc_7543p_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4910
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4911
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4912
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4913

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4914
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4915
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4916
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4917
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4918
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26330**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4920
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4921
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4922
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4924
epyc_7543_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4925
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4926
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4928
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4929
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4930
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4931
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4933
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4934
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4935
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4936
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2021-26335**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4938
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4939
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4940
epyc_7551p_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**		
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4942
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4943
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4944
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4945
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26330**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4947
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4948
epyc_7551_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4949
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/4950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	e/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4951
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4952
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4953
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4954
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/4955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	etin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4956
epyc_7552_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4957
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4958
Improper Neutralization of Special	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/4959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	e/product-security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4960
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4961
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4962
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4963
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/4964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	etin/amd-sb-1021	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4965
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4966
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4967
epyc_75f3_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	sb-1021	
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4969
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4970
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4971
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4972

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack”. **CVE ID : CVE-2021-26322**	security/bulletin/amd-sb-1021	
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4973
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4974
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4975
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4976
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4978
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4979
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4980
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4981
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/4982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	etin/amd-sb-1021	
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4983
epyc_7601_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4984
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4985
Improper Neutralization of Special Elements	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4987
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4988
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4989
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4990
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/4991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	sb-1021	
epyc_7642_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4992
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4993
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4994
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/4995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack”. **CVE ID : CVE-2021-26322**	security/bulletin/amd-sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4996
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4997
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4998
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/4999
Improper Restriction of	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/5000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5001
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5002
epyc_7643_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5003
Insufficient	16-Nov-21	4.6	When the AMD Platform	https://ww	O-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Verification of Data Authenticity			Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	w.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	081221/5004
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5005
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5006
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5007
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity.	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/5008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26323	etin/amd-sb-1021	
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5009
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5010
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5011
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5012
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5013
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a	https://www.amd.com/	O-AMD-EPYC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	en/corporate/product-security/bulletin/amd-sb-1021	081221/5014
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5015
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5016
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5017
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/5018

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potential lack of system resources. **CVE ID : CVE-2021-26338**	sb-1021	
epyc_7662_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5019
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5020
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5021
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”.	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/5022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26322	etin/amd-sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5023
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5024
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5025
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5026
Improper Restriction of Operations	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/5027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5028
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5029
epyc_7663_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5030
Insufficient Verification	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot	https://www.amd.com/	O-AMD-EPYC-081221/5031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Data Authenticity			rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	en/corporate/product-security/bulletin/amd-sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5032
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5033
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5034
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/5035

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5036
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5037
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5038
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5039
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5040
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/5041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	e/product-security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5042
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5043
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5044
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/5045

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26338**	sb-1021	
epyc_7702p_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5046
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5047
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5048
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/5049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5050
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5051
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5052
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5053
Improper Restriction of Operations within the	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/5054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	etin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5055
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5056
epyc_7702_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5057
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/5058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	e/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5059
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5060
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5061
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5062
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/5063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	etin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5064
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5065
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5066
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26338		
epyc_7713p_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5068
Insufficient Verification of Data Authenticity	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5069
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5070
Improper Neutralization of Special	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/5071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	e/product-security/bulletin/amd-sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5072
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5073
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5074
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5075
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/5076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5077
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5078
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5079
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5080
Improper Restriction of Operations within the	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/5081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	etin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5082
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5083
epyc_7713_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5084
Insufficient Verification of Data	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/5085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authenticity			subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	e/product-security/bulletin/amd-sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5086
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5087
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5088
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5090
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5091
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5092
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5093
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5094
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/5095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5096
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5097
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5098
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26338**		
epyc_7742_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5100
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5101
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5102
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/5103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5104
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5105
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5106
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5107
Improper Restriction of Operations within the	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/5108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	etin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5109
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5110
epyc_7763_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5111
Insufficient Verification of Data	16-Nov-21	4.6	When the AMD Platform Security Processor (PSP) boot rom loads, authenticates, and	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/5112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authenticity			subsequently decrypts an encrypted FW, due to insufficient verification of the integrity of decrypted image, arbitrary code may be executed in the PSP when encrypted firmware images are used. **CVE ID : CVE-2021-26315**	e/product-security/bulletin/amd-sb-1021	
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5113
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5114
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5115
Improper Input Validation	16-Nov-21	4.6	Failure to validate SEV Commands while SNP is active may result in a potential impact to memory integrity. **CVE ID : CVE-2021-26323**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Nov-21	2.1	Insufficient input validation in the SNP_GUEST_REQUEST command may lead to a potential data abort error and a denial of service. **CVE ID : CVE-2021-26325**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5117
Improper Initialization	16-Nov-21	7.2	Failure to validate VM_HSAVE_PA during SNP_INIT may result in a loss of memory integrity. **CVE ID : CVE-2021-26326**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5118
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	Insufficient validation of guest context in the SNP Firmware could lead to a potential loss of guest confidentiality. **CVE ID : CVE-2021-26327**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5119
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5120
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5121
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-081221/5122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	security/bulletin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5123
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5124
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5125
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources. **CVE ID : CVE-2021-26338**		
epyc_7f32_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5127
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5128
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5129
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/5130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sb-1021	
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5131
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5132
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5133
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5134
Improper Restriction of Operations within the	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/5135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	etin/amd-sb-1021	
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5136
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5137
epyc_7f52_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5138
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command	https://www.amd.com/en/corporat	O-AMD-EPYC-081221/5139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	e/product-security/bulletin/amd-sb-1021	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5140
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5141
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5142
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5143
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries	https://www.amd.com/en/corporate/product-security/bull	O-AMD-EPYC-081221/5144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	etin/amd-sb-1021	
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5145
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	4.9	Insufficient bounds checking in System Management Unit (SMU) may cause invalid memory accesses/updates that could result in SMU hang and subsequent failure to service any further requests from other components. **CVE ID : CVE-2021-26336**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5146
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests. **CVE ID : CVE-2021-26337**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5147
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26338		
epyc_7f72_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5149
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5150
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP. **CVE ID : CVE-2021-26321**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5151
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential “two time pad attack”. **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5153
Out-of-bounds Write	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience a heap-based overflow which may result in a loss of resources. **CVE ID : CVE-2021-26330**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5154
N/A	16-Nov-21	7.2	AMD System Management Unit (SMU) contains a potential issue where a malicious user may be able to manipulate mailbox entries leading to arbitrary code execution. **CVE ID : CVE-2021-26331**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5155
N/A	16-Nov-21	7.2	Improper input and range checking in the Platform Security Processor (PSP) boot loader image header may allow for an attacker to use attack-controlled values prior to signature validation potentially resulting in arbitrary code execution. **CVE ID : CVE-2021-26335**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5156
N/A	16-Nov-21	2.1	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA read from invalid DRAM address to SRAM resulting in SMU not servicing further requests.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5157

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26337		
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5158
epyc_7h12_firmware					
Exposure of Resource to Wrong Sphere	16-Nov-21	2.1	PSP protection against improperly configured side channels may lead to potential information disclosure. This issue affects: AMD 1st Gen AMD EPYC™ versions prior to NaplesPI-SP3_1.0.0.G. AMD 2nd Gen AMD EPYC™ versions prior to RomePI-SP3_1.0.0.C. AMD 3rd Gen AMD EPYC™ versions prior to MilanPI-SP3_1.0.0.4. **CVE ID : CVE-2021-26312**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5159
Improper Certificate Validation	16-Nov-21	2.1	Insufficient validation of the AMD SEV Signing Key (ASK) in the SEND_START command in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP **CVE ID : CVE-2021-26320**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5160
Improper Neutralization of Special Elements used in a Command	16-Nov-21	4.9	Insufficient ID command validation in the SEV Firmware may allow a local authenticated attacker to perform a denial of service of the PSP.	https://www.amd.com/en/corporate/product-security/bulletin/amd-	O-AMD-EPYC-081221/5161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			**CVE ID : CVE-2021-26321**	sb-1021	
Use of Insufficiently Random Values	16-Nov-21	5	Persistent platform private key may not be protected with a random IV leading to a potential "two time pad attack". **CVE ID : CVE-2021-26322**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5162
Integer Overflow or Wraparound	16-Nov-21	2.1	AMD System Management Unit (SMU) may experience an integer overflow when an invalid length is provided which may result in a potential loss of resources. **CVE ID : CVE-2021-26329**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5163
N/A	16-Nov-21	7.8	Improper access controls in System Management Unit (SMU) may allow for an attacker to override performance control tables located in DRAM resulting in a potential lack of system resources. **CVE ID : CVE-2021-26338**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1021	O-AMD-EPYC-081221/5164
Apple					
macos					
Improper Resource Shutdown or Release	26-Nov-21	4.3	A vulnerability affecting F-Secure antivirus engine was discovered whereby unpacking UPX file can lead to denial-of-service. The vulnerability can be exploited remotely by an attacker. A successful attack will result in denial-of-service of the antivirus engine. **CVE ID : CVE-2021-40833**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-	O-APP-MACO-081221/5165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40833	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Nov-21	9.3	Adobe InDesign versions 16.4 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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-2021-42731**	https://helpx.adobe.com/security/products/indesign/apsb21-107.html	O-APP-MACO-081221/5166
Access of Memory Location After End of Buffer	16-Nov-21	9.3	Adobe Media Encoder version 15.4.1 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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-2021-43013**	https://helpx.adobe.com/security/products/media-encoder/apsb21-99.html	O-APP-MACO-081221/5167
Access of	22-Nov-21	9.3	Adobe InCopy version 16.4	https://help	O-APP-MACO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Location After End of Buffer			(and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious GIF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-43015**	x.adobe.com /security/pr oducts/inco py/apsb21-110.html	081221/5168
NULL Pointer Dereference	22-Nov-21	4.3	Adobe InCopy version 16.4 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2021-43016**	https://help x.adobe.com /security/pr oducts/inco py/apsb21-110.html	O-APP-MACO-081221/5169
N/A	18-Nov-21	3.5	Adobe Creative Cloud version 5.5 (and earlier) are affected by an Application denial of service vulnerability in the Creative Cloud Desktop installer. An authenticated attacker could leverage this vulnerability to achieve denial of service in the context of the user. User interaction is required before product installation to abuse this	https://help x.adobe.com /security/pr oducts/creat ive-cloud/apsb2 1-111.html	O-APP-MACO-081221/5170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. **CVE ID : CVE-2021-43017**		
Improper Access Control	23-Nov-21	9.3	Adobe Creative Cloud version 5.5 (and earlier) are affected by a privilege escalation vulnerability in the resources leveraged by the Setup.exe service. An unauthenticated attacker could leverage this vulnerability to remove files and escalate privileges under the context of SYSTEM . An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability on the product installer. User interaction is required before product installation to abuse this vulnerability. **CVE ID : CVE-2021-43019**	https://helpx.adobe.com/security/products/creative-cloud/apsb21-111.html, https://www.zerodayinitiative.com/advisories/ZDI-21-1333/	O-APP-MACO-081221/5171
Asus					
gt-ax11000_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-	O-ASU-GT-A-081221/5172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-GT-A-081221/5173
rt-ax3000_firmware					
Improper Restriction of Excessive Authenticati	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-	https://www.asus.com/Networking-IoT-	O-ASU-RT-A-081221/5174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on Attempts			AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-	O-ASU-RT-A-081221/5175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	AX3000/HelpDesk_BIOS/, http://asus.com	
rt-ax55_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-RT-A-081221/5176
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION,	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-	O-ASU-RT-A-081221/5177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
rt-ax56u_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/,	O-ASU-RT-A-081221/5178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-RT-A-081221/5179
rt-ax56u_v2_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://ww	O-ASU-RT-A-081221/5180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	w.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-RT-A-081221/5181
rt-ax58u_firmware					
Improper	19-Nov-21	10	A brute-force protection	https://ww	O-ASU-RT-A-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Excessive Authentication Attempts			bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	w.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	081221/5182
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-	O-ASU-RT-A-081221/5183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
rt-ax68u_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-RT-A-081221/5184
Inconsistent Interpretation of HTTP Requests ('HTTP Request	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U	https://www.asus.com/Networking-IoT-Servers/WiFi-	O-ASU-RT-A-081221/5185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Smuggling')			GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
rt-ax82u_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-	O-ASU-RT-A-081221/5186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-RT-A-081221/5187
rt-ax82u_gundam_edition_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-	O-ASU-RT-A-081221/5188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.c	O-ASU-RT-A-081221/5189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om	
rt-ax86s_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-RT-A-081221/5190
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/	O-ASU-RT-A-081221/5191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
rt-ax86u_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-RT-A-081221/5192
Inconsistent Interpretatio	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS	https://www.asus.com/	O-ASU-RT-A-081221/5193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of HTTP Requests ('HTTP Request Smuggling')			ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
rt-ax86u_zaku_ii_edition_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiF	O-ASU-RT-A-081221/5194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	i-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-RT-A-081221/5195
rt-ax88u_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U,	https://www.asus.com/Networking-IoT-Servers/WiF	O-ASU-RT-A-081221/5196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	i-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet.	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/Hel	O-ASU-RT-A-081221/5197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-41436	pDesk_BIOS/, http://asus.com	
rt-ax92u_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-RT-A-081221/5198
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/Help	O-ASU-RT-A-081221/5199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	Desk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
tuf-ax5400_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.c	O-ASU-TUF--081221/5200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-TUF--081221/5201
tuf_gaming_ax3000_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/	O-ASU-TUF_-081221/5202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-TUF_-081221/5203
zenwifi_ax_\\(xt8\\)_firmware					
Improper Restriction	19-Nov-21	10	A brute-force protection bypass in CAPTCHA	https://www.asus.com/	O-ASU-ZENW-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Excessive Authentication Attempts			protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	081221/5204
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/AS	O-ASU-ZENW-081221/5205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	US-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
zenwifi_xd6_firmware					
Improper Restriction of Excessive Authentication Attempts	19-Nov-21	10	A brute-force protection bypass in CAPTCHA protection in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86 Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote attacker to attempt any number of login attempts via sending a specific HTTP request. **CVE ID : CVE-2021-41435**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	O-ASU-ZENW-081221/5206
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Nov-21	7.8	An HTTP request smuggling in web application in ASUS ROG Rapture GT-AX11000, RT-AX3000, RT-AX55, RT-AX56U, RT-AX56U_V2, RT-AX58U, RT-AX82U, RT-AX82U GUNDAM EDITION, RT-AX86	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/AS	O-ASU-ZENW-081221/5207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series(RT-AX86U/RT-AX86S), RT-AX86U ZAKU II EDITION, RT-AX88U, RT-AX92U, TUF Gaming AX3000, TUF Gaming AX5400 (TUF-AX5400), ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) before 3.0.0.4.386.45898, and RT-AX68U before 3.0.0.4.386.45911, allows a remote unauthenticated attacker to DoS via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41436**	US-WiFi-Routers/RT-AX56U/HelpDesk_BIOS/, https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/HelpDesk_BIOS/, http://asus.com	
Canonical					
ubuntu_linux					
Release of Invalid Pointer or Reference	17-Nov-21	7.2	Ubuntu-specific modifications to accountsservice (in patch file debian/patches/0010-set-language.patch) caused the fallback_locale variable, pointing to static storage, to be freed, in the user_change_language_authorized_cb function. This is reachable via the SetLanguage dbus function. This is fixed in versions 0.6.55-0ubuntu12~20.04.5, 0.6.55-0ubuntu13.3, 0.6.55-0ubuntu14.1. **CVE ID : CVE-2021-3939**	https://ubuntu.com/security/notices/USN-5149-1	O-CAN-UBUN-081221/5208
Debian					
debian_linux					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Nov-21	4.3	Roundcube before 1.3.17 and 1.4.x before 1.4.12 is prone to XSS in handling an attachment's filename extension when displaying a MIME type warning message. **CVE ID : CVE-2021-44025**	https://github.com/roundcube/roundcubemail/commit/7d7b1dfeff795390b69905ceb63d6391b5b0dfe7, https://github.com/roundcube/roundcubemail/issues/8193, https://github.com/roundcube/roundcubemail/commit/faf99bf8a2b7b7562206fa047e8de652861e624a	O-DEB-DEBI-081221/5209
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Nov-21	7.5	Roundcube before 1.3.17 and 1.4.x before 1.4.12 is prone to a potential SQL injection via search or search_params. **CVE ID : CVE-2021-44026**	https://github.com/roundcube/roundcubemail/commit/ee809bde2dcaa04857a919397808a7296681dcfa, https://github.com/roundcube/roundcubemail/commit/c8947ecb762d9e89c2091bda28d490028	O-DEB-DEBI-081221/5210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				17263f1	
Out-of-bounds Write	22-Nov-21	7.5	A flaw was found in mbsync in isync 1.4.0 through 1.4.3. Due to an unchecked condition, a malicious or compromised IMAP server could use a crafted mail message that lacks headers (i.e., one that starts with an empty line) to provoke a heap overflow, which could conceivably be exploited for remote code execution. **CVE ID : CVE-2021-44143**	https://sourceforge.net/p/isync/isync/commit_browser	O-DEB-DEBI-081221/5211
Dell					
emc_idrac8_firmware					
Out-of-bounds Write	23-Nov-21	6.5	Dell iDRAC 9 prior to version 4.40.40.00 and iDRAC 8 prior to version 2.80.80.80 contain a Stack Buffer Overflow in Racadm. An authenticated remote attacker may potentially exploit this vulnerability to control process execution and gain access to the underlying operating system. **CVE ID : CVE-2021-36301**	https://support.emc.com/kb/000191229	O-DEL-EMC_-081221/5212
emc_idrac9_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Nov-21	5.5	Dell iDRAC9 versions 4.40.00.00 and later, but prior to 4.40.29.00 and 5.00.00.00 contain an SQL injection vulnerability. A remote authenticated malicious user with low privileges may potentially exploit this vulnerability to cause	https://support.emc.com/kb/000191229	O-DEL-EMC_-081221/5213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure or denial of service by supplying specially crafted input data to the affected application. **CVE ID : CVE-2021-36299**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Nov-21	6.4	iDRAC9 versions prior to 5.00.00.00 contain an improper input validation vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability by sending a specially crafted malicious request to crash the webserver or cause information disclosure. **CVE ID : CVE-2021-36300**	https://support.emc.com/kb/000191229	O-DEL-EMC_-081221/5214
Out-of-bounds Write	23-Nov-21	6.5	Dell iDRAC 9 prior to version 4.40.40.00 and iDRAC 8 prior to version 2.80.80.80 contain a Stack Buffer Overflow in Racadm. An authenticated remote attacker may potentially exploit this vulnerability to control process execution and gain access to the underlying operating system. **CVE ID : CVE-2021-36301**	https://support.emc.com/kb/000191229	O-DEL-EMC_-081221/5215
emc_powerscale_onefs					
Insertion of Sensitive Information into Log File	23-Nov-21	2.1	Dell PowerScale OneFS version 8.1.2 contains a sensitive information exposure vulnerability. This would allow a malicious user with ISI_PRIV_LOGIN_SSH and/or ISI_PRIV_LOGIN_CONSOLE privileges to gain access to	https://www.dell.com/support/kbdoc/000191265	O-DEL-EMC_-081221/5216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive information in the log files. **CVE ID : CVE-2021-21561**		
networking_os10					
Improper Authentication	20-Nov-21	9.3	Networking OS10, versions prior to October 2021 with RESTCONF API enabled, contains an authentication bypass vulnerability. A remote unauthenticated attacker could exploit this vulnerability to gain access and perform actions on the affected system. **CVE ID : CVE-2021-36306**	https://www.dell.com/support/kbdoc/en-us/000193076	O-DEL-NETW-081221/5217
Improper Privilege Management	20-Nov-21	8.5	Networking OS10, versions prior to October 2021 with RESTCONF API enabled, contains a privilege escalation vulnerability. A malicious low privileged user with specific access to the API could potentially exploit this vulnerability to gain admin privileges on the affected system. **CVE ID : CVE-2021-36307**	https://www.dell.com/support/kbdoc/en-us/000193076	O-DEL-NETW-081221/5218
Authentication Bypass Using an Alternate Path or Channel	20-Nov-21	9.3	Networking OS10, versions prior to October 2021 with Smart Fabric Services enabled, contains an authentication bypass vulnerability. A remote unauthenticated attacker could exploit this vulnerability to gain access and perform actions on the affected system.	https://www.dell.com/support/kbdoc/en-us/000193076	O-DEL-NETW-081221/5219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36308		
Uncontrolled Resource Consumption	20-Nov-21	6.8	Dell Networking OS10, versions 10.4.3.x, 10.5.0.x, 10.5.1.x & 10.5.2.x, contain an uncontrolled resource consumption flaw in its API service. A high-privileged API user may potentially exploit this vulnerability, leading to a denial of service. **CVE ID : CVE-2021-36310**	https://www.dell.com/support/kbdoc/en-us/000193076	O-DEL-NETW-081221/5220
Exposure of Resource to Wrong Sphere	20-Nov-21	2.1	Dell Networking OS10 versions 10.4.3.x, 10.5.0.x and 10.5.1.x contain an information exposure vulnerability. A low privileged authenticated malicious user can gain access to SNMP authentication failure messages. **CVE ID : CVE-2021-36319**	https://www.dell.com/support/kbdoc/en-us/000193076	O-DEL-NETW-081221/5221
x1008p_firmware					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X100-081221/5222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X100-081221/5223
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X100-081221/5224
x1008_firmware					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-	O-DEL-X100-081221/5225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X100-081221/5226
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabiliti	O-DEL-X100-081221/5227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				es	
x1018p_firmware					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X101-081221/5228
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X101-081221/5229
Improper Neutralization of Special Elements in Output Used by a	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-	O-DEL-X101-081221/5230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Downstream Component ('Injection')			exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	
x1018_firmware					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X101-081221/5231
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-	O-DEL-X101-081221/5232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				security-vulnerabilities	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X101-081221/5233
x1026p_firmware					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X102-081221/5234
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability.	https://www.dell.com/support/kbdoc/en-	O-DEL-X102-081221/5235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X102-081221/5236
x1026_firmware					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-	O-DEL-X102-081221/5237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				update-for-multiple-security-vulnerabilities	
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X102-081221/5238
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X102-081221/5239
x1052p_firmware					
Insufficient	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to	https://www.dell.com/s	O-DEL-X105-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Entropy			3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	upport/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	081221/5240
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X105-081221/5241
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-	O-DEL-X105-081221/5242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			redirections. **CVE ID : CVE-2021-36322**	security-update-for-multiple-security-vulnerabilities	
x1052_firmware					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X105-081221/5243
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X105-081221/5244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X105-081221/5245
x4012_firmware					
Insufficient Entropy	20-Nov-21	7.5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an authentication bypass vulnerability. A remote unauthenticated attacker may potentially hijack a session and access the webserver by forging the session ID. **CVE ID : CVE-2021-36320**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X401-081221/5246
Improper Input Validation	20-Nov-21	5	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain an improper input validation vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-	O-DEL-X401-081221/5247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted data to trigger a denial of service. **CVE ID : CVE-2021-36321**	dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-21	5.8	Dell Networking X-Series firmware versions prior to 3.0.1.8 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary host header values to poison the web-cache or trigger redirections. **CVE ID : CVE-2021-36322**	https://www.dell.com/support/kbdoc/en-us/000193230/dsa-2021-191-dell-networking-x-series-security-update-for-multiple-security-vulnerabilities	O-DEL-X401-081221/5248
Dlink					
dwr-932c_e1_firmware					
Missing Authentication for Critical Function	23-Nov-21	10	Missing Authentication for Critical Function vulnerability in debug_post_set.cgi of D-Link DWR-932C E1 firmware allows an unauthenticated attacker to execute administrative actions. **CVE ID : CVE-2021-42783**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10246	O-DLI-DWR--081221/5249
Improper Neutralization of Special Elements	23-Nov-21	10	OS Command Injection vulnerability in debug_fcgi of D-Link DWR-932C E1 firmware allows a remote	https://supportannouncement.us.dlink.com/anno	O-DLI-DWR--081221/5250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attacker to perform command injection via a crafted HTTP request. **CVE ID : CVE-2021-42784**	uncement/publication.aspx?name=SAP10246	
Fedoraproject					
fedora					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**	https://c-ares.haxx.se/adv_20210810.html	O-FED-FEDO-081221/5251
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Nov-21	5.1	When PgBouncer is configured to use "cert" authentication, a man-in-the-middle attacker can inject arbitrary SQL queries when a connection is first established, despite the use of TLS certificate verification and encryption. This flaw affects PgBouncer versions prior to 1.16.1. **CVE ID : CVE-2021-3935**	http://www.pgbouncer.org/changelog.html#pgbouncer-116x	O-FED-FEDO-081221/5252
Out-of-bounds Write	19-Nov-21	8.5	vim is vulnerable to Heap-based Buffer Overflow **CVE ID : CVE-2021-3968**	https://huntr.dev/bounties/00d62924-a7b4-4a61-ba29-acab2eaa1528,	O-FED-FEDO-081221/5253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://github.com/vim/vim/commit/a062006b9de0b2947ab5fb376c6e67ef92a8cd69	
Out-of-bounds Write	19-Nov-21	9.3	vim is vulnerable to Heap-based Buffer Overflow **CVE ID : CVE-2021-3973**	https://github.com/vim/vim/commit/615ddd5342b50a6878a907062aa471740bd9a847, https://huntr.dev/bounties/ce6e8609-77c6-4e17-b9fc-a2e5abed052e	O-FED-FEDO-081221/5254
Use After Free	19-Nov-21	6.8	vim is vulnerable to Use After Free **CVE ID : CVE-2021-3974**	https://github.com/vim/vim/commit/64066b9acd9f8cffdf4840f797748f938a13f2d6, https://huntr.dev/bounties/e402cb2c-8ec4-4828-a692-c95f8e0de6d4	O-FED-FEDO-081221/5255
Access of Resource Using	17-Nov-21	4	The OCI Distribution Spec project defines an API protocol to facilitate and	https://github.com/opencontainers/	O-FED-FEDO-081221/5256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incompatible Type ('Type Confusion')			standardize the distribution of content. In the OCI Distribution Specification version 1.0.0 and prior, the Content-Type header alone was used to determine the type of document during push and pull operations. Documents that contain both “manifests” and “layers” fields could be interpreted as either a manifest or an index in the absence of an accompanying Content-Type header. If a Content-Type header changed between two pulls of the same digest, a client may interpret the resulting content differently. The OCI Distribution Specification has been updated to require that a mediaType value present in a manifest or index match the Content-Type header used during the push and pull operations. Clients pulling from a registry may distrust the Content-Type header and reject an ambiguous document that contains both “manifests” and “layers” fields or “manifests” and “config” fields if they are unable to update to version 1.0.1 of the spec. **CVE ID : CVE-2021-41190**	distribution-spec/security/advisories/GHSA-mc8v-mgrf-8f4m, https://github.com/opencontainers/distribution-spec/commit/ac28cac0557bcd3084714ab09f9f2356fe504923	
Incorrect Authorization	17-Nov-21	4	SchedMD Slurm 21.08.* before 21.08.4 has Incorrect Access Control. On sites using the new	https://lists.schedmd.com/pipermail/slurm-	O-FED-FEDO-081221/5257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AccountingStoreFlags=job_script and/or job_env options, the access control rules in SlurmDBD may permit users to request job scripts and environment files to which they should not have access. **CVE ID : CVE-2021-43337**	announce/, https://www.schedmd.com/news.php, https://www.schedmd.com/news.php?id=256, https://lists.schedmd.com/pipermail/slurm-announce/2021/000068.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-21	4.3	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. A URL parameter in the filetype site administrator tool required extra sanitizing to prevent a reflected XSS risk. **CVE ID : CVE-2021-43558**	https://moodle.org/mod/forum/discuss.php?d=429097	O-FED-FEDO-081221/5258
Cross-Site Request Forgery (CSRF)	22-Nov-21	6.8	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. The "delete related badge" functionality did not include the necessary token check to prevent a CSRF risk. **CVE ID : CVE-2021-43559**	https://moodle.org/mod/forum/discuss.php?d=429099	O-FED-FEDO-081221/5259
Exposure of Resource to Wrong Sphere	22-Nov-21	5	A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions.	https://moodle.org/mod/forum/discuss.php?d=4	O-FED-FEDO-081221/5260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Insufficient capability checks made it possible to fetch other users' calendar action events. **CVE ID : CVE-2021-43560**	29100	
Out-of-bounds Write	17-Nov-21	4.6	In the Linux kernel through 5.15.2, hw_atl_utils_fw_rpc_wait in drivers/net/ethernet/aquantia/atlantic/hw_atl/hw_atl_utils.c allows an attacker (who can introduce a crafted device) to trigger an out-of-bounds write via a crafted length value. **CVE ID : CVE-2021-43975**	https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=b922f622592af76b57cbc566eaeccda0b31a3496, https://lore.kernel.org/netdev/163698540868.13805.178004080217824087 62.git-patchwork-notify@kernel.org/T/	O-FED-FEDO-081221/5261
N/A	17-Nov-21	2.1	In the Linux kernel through 5.15.2, mwifiex_usb_recv in drivers/net/wireless/marvell/mwifiex/usb.c allows an attacker (who can connect a crafted USB device) to cause a denial of service (skb_over_panic). **CVE ID : CVE-2021-43976**	https://patchwork.kernel.org/project/linux-wireless/patch/YX4CqjfRcTa6bVL+@Zekuns-MBP-16.fios-router.home/	O-FED-FEDO-081221/5262
Improper Neutralization of Input During Web	19-Nov-21	4.3	Roundcube before 1.3.17 and 1.4.x before 1.4.12 is prone to XSS in handling an attachment's filename	https://github.com/roundcube/roundcubemail/	O-FED-FEDO-081221/5263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			extension when displaying a MIME type warning message. **CVE ID : CVE-2021-44025**	commit/7d7b1dfeff795390b69905ceb63d6391b5b0dfe7, https://github.com/roundcube/roundcubemail/issues/8193, https://github.com/roundcube/roundcubemail/commit/faf99bf8a2b7b7562206fa047e8de652861e624a	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Nov-21	7.5	Roundcube before 1.3.17 and 1.4.x before 1.4.12 is prone to a potential SQL injection via search or search_params. **CVE ID : CVE-2021-44026**	https://github.com/roundcube/roundcubemail/commit/ee809bde2dcaa04857a919397808a7296681dcfa, https://github.com/roundcube/roundcubemail/commit/c8947ecb762d9e89c2091bda28d49002817263f1	O-FED-FEDO-081221/5264
N/A	18-Nov-21	5	A flaw was discovered in Puppet Agent and Puppet Server that may result in a	https://puppet.com/security/cve/C	O-FED-FEDO-081221/5265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leak of HTTP credentials when following HTTP redirects to a different host. This is similar to CVE-2018-1000007 **CVE ID : CVE-2021-27023**	VE-2021-27023	
N/A	18-Nov-21	4	A flaw was discovered in Puppet Agent where the agent may silently ignore Augeas settings or may be vulnerable to a Denial of Service condition prior to the first 'pluginsync'. **CVE ID : CVE-2021-27025**	https://puppet.com/security/cve/cve-2021-27025	O-FED-FEDO-081221/5266
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-21	6.9	PoD operations on misaligned GFNs T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] x86 HVM and PVH guests may be started in populate-on-demand (PoD) mode, to provide a way for them to later easily have more memory assigned. Guests are permitted to control certain P2M aspects of individual pages via hypercalls. These hypercalls may act on ranges of pages specified via page orders (resulting in a power-of-2 number of pages). The implementation of some of these hypercalls for PoD does not enforce the base page frame number to be suitably aligned for the specified order, yet some code involved in PoD handling actually	https://xenbits.xenproject.org/xsa/advisory-388.txt	O-FED-FEDO-081221/5267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			makes such an assumption. These operations are XENMEM_decrease_reservation (CVE-2021-28704) and XENMEM_populate_physmap (CVE-2021-28707), the latter usable only by domains controlling the guest, i.e. a de-privileged qemu or a stub domain. (Patch 1, combining the fix to both these two issues.) In addition handling of XENMEM_decrease_reservation can also trigger a host crash when the specified page order is neither 4k nor 2M nor 1G (CVE-2021-28708, patch 2). **CVE ID : CVE-2021-28704**		
Fortinet					
fortios					
N/A	17-Nov-21	2.1	An exposure of sensitive information to an unauthorized actor vulnerability in FortiOS CLI 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, 6.0.x and 5.6.x may allow a local and authenticated user assigned to a specific VDOM to retrieve other VDOMs information such as the admin account list and the network interface list. **CVE ID : CVE-2021-32600**	https://fortiguard.com/advisory/FG-IR-20-243	O-FOR-FORT-081221/5268
Google					
android					
Improper Input	23-Nov-21	5.8	Insufficient validation of untrusted input in Intents in	https://crbug.com/1249	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Google Chrome on Android prior to 95.0.4638.69 allowed a remote attacker to arbitrarily browser to a malicious URL via a crafted HTML page. **CVE ID : CVE-2021-38000**	962, https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html	081221/5269
Out-of-bounds Read	18-Nov-21	2.1	In ape extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561395; Issue ID: ALPS05561395. **CVE ID : CVE-2021-0619**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5270
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561381. **CVE ID : CVE-2021-0620**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5271
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/Nov	O-GOO-ANDR-081221/5272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561383. **CVE ID : CVE-2021-0621**	ember-2021	
Out-of-bounds Read	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05561388. **CVE ID : CVE-2021-0622**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5273
Integer Overflow or Wraparound	18-Nov-21	2.1	In asf extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05585817. **CVE ID : CVE-2021-0623**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5274
Out-of-bounds Read	18-Nov-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05594988; Issue ID: ALPS05594988. **CVE ID : CVE-2021-0624**		
Use After Free	18-Nov-21	7.2	In mdlactl driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05776625; Issue ID: ALPS05776625. **CVE ID : CVE-2021-0629**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5276
Improper Privilege Management	18-Nov-21	4.6	In mdlactl driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05673424; Issue ID: ALPS05673424. **CVE ID : CVE-2021-0655**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5277
Use After Free	18-Nov-21	4.6	In edma driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05709376; Issue ID: ALPS05709376. **CVE ID : CVE-2021-0656**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5278
Out-of-bounds	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a	https://corp.mediatek.co	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672103; Issue ID: ALPS05672103. **CVE ID : CVE-2021-0657**	m/product-security-bulletin/November-2021	081221/5279
Out-of-bounds Write	18-Nov-21	4.6	In apusys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672107; Issue ID: ALPS05672107. **CVE ID : CVE-2021-0658**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5280
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05687559; Issue ID: ALPS05687559. **CVE ID : CVE-2021-0659**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5281
Use After Free	18-Nov-21	4.6	In ccu, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05827158; Issue ID: ALPS05827158. **CVE ID : CVE-2021-0664**		
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672113; Issue ID: ALPS05672113. **CVE ID : CVE-2021-0665**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5283
Out-of-bounds Read	18-Nov-21	2.1	In apusys, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05672086; Issue ID: ALPS05672086. **CVE ID : CVE-2021-0666**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5284
Use After Free	18-Nov-21	4.6	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670581; Issue ID: ALPS05670581. **CVE ID : CVE-2021-0667**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5285
Improper Handling of Exceptional	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to incorrect error handling. This	https://corp.mediatek.com/product-	O-GOO-ANDR-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conditions			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05670521; Issue ID: ALPS05670521. **CVE ID : CVE-2021-0668**	security-bulletin/November-2021	081221/5286
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05681550; Issue ID: ALPS05681550. **CVE ID : CVE-2021-0669**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5287
Use After Free	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05654663; Issue ID: ALPS05654663. **CVE ID : CVE-2021-0670**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5288
Out-of-bounds Write	18-Nov-21	7.2	In apusys, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05664273; Issue ID:	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05664273. **CVE ID : CVE-2021-0671**		
Incorrect Default Permissions	18-Nov-21	2.1	In Browser app, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05969704; Issue ID: ALPS05969704. **CVE ID : CVE-2021-0672**	https://corp.mediatek.com/product-security-bulletin/November-2021	O-GOO-ANDR-081221/5290
hej					
hejhome_gkw-ic052_firmware					
Use of Hard-coded Credentials	26-Nov-21	7.5	HejHome GKW-IC052 IP Camera contained a hard-coded credentials vulnerability. This issue allows remote attackers to operate the IP Camera.(reboot, factory reset, snapshot etc..) **CVE ID : CVE-2021-26611**	N/A	O-HEJ-HEJH-081221/5291
Hitachi					
gms600_firmware					
Incorrect Authorization	18-Nov-21	9	Insufficient security control vulnerability in internal database access mechanism of Hitachi Energy Relion 670/650/SAM600-IO, Relion 650, GMS600, PWC600 allows attacker who successfully exploited this vulnerability, of which the product does not sufficiently restrict access to an internal database tables,	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000059&LanguageCode=en&DocumentPartId=&Action=Launch,	O-HIT-GMS6-081221/5292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow anybody with user credentials to bypass security controls that is enforced by the product. Consequently, exploitation may lead to unauthorized modifications on data/firmware, and/or to permanently disabling the product. This issue affects: Hitachi Energy Relion 670 Series 2.0 all revisions; 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.5. Hitachi Energy Relion 670/650 Series 2.1 all revisions. 2.2.0 all revisions; 2.2.4 all revisions; Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions; 2.2.5 versions prior to 2.2.5.2. Hitachi Energy Relion 650 1.0 all revisions. 1.1 all revisions; 1.2 all revisions; 1.3 versions prior to 1.3.0.8; Hitachi Energy GMS600 1.3.0; 1.3.0.1; 1.2.0. Hitachi Energy PWC600 1.0.1 version 1.0.1.4 and prior versions; 1.1.0 version 1.1.0.1 and prior versions. **CVE ID : CVE-2021-35534**	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000058&LanguageCode=en&DocumentPartId=&Action=Launch	
pwc600_firmware					
Incorrect Authorization	18-Nov-21	9	Insufficient security control vulnerability in internal database access mechanism of Hitachi Energy Relion 670/650/SAM600-IO, Relion 650, GMS600, PWC600 allows attacker who successfully exploited this vulnerability, of	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000059&LanguageCode=en&D	O-HIT-PWC6-081221/5293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which the product does not sufficiently restrict access to an internal database tables, could allow anybody with user credentials to bypass security controls that is enforced by the product. Consequently, exploitation may lead to unauthorized modifications on data/firmware, and/or to permanently disabling the product. This issue affects: Hitachi Energy Relion 670 Series 2.0 all revisions; 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.5. Hitachi Energy Relion 670/650 Series 2.1 all revisions. 2.2.0 all revisions; 2.2.4 all revisions; Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions; 2.2.5 versions prior to 2.2.5.2. Hitachi Energy Relion 650 1.0 all revisions. 1.1 all revisions; 1.2 all revisions; 1.3 versions prior to 1.3.0.8; Hitachi Energy GMS600 1.3.0; 1.3.0.1; 1.2.0. Hitachi Energy PWC600 1.0.1 version 1.0.1.4 and prior versions; 1.1.0 version 1.1.0.1 and prior versions. **CVE ID : CVE-2021-35534**	ocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000058&LanguageCode=en&DocumentPartId=&Action=Launch	
relion_650_firmware					
Incorrect Authorization	18-Nov-21	9	Insufficient security control vulnerability in internal database access mechanism of Hitachi Energy Relion 670/650/SAM600-IO, Relion	https://search.abb.com/library/Download.aspx?DocumentID	O-HIT-RELI-081221/5294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650, GMS600, PWC600 allows attacker who successfully exploited this vulnerability, of which the product does not sufficiently restrict access to an internal database tables, could allow anybody with user credentials to bypass security controls that is enforced by the product. Consequently, exploitation may lead to unauthorized modifications on data/firmware, and/or to permanently disabling the product. This issue affects: Hitachi Energy Relion 670 Series 2.0 all revisions; 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.5. Hitachi Energy Relion 670/650 Series 2.1 all revisions. 2.2.0 all revisions; 2.2.4 all revisions; Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions; 2.2.5 versions prior to 2.2.5.2. Hitachi Energy Relion 650 1.0 all revisions. 1.1 all revisions; 1.2 all revisions; 1.3 versions prior to 1.3.0.8; Hitachi Energy GMS600 1.3.0; 1.3.0.1; 1.2.0. Hitachi Energy PWC600 1.0.1 version 1.0.1.4 and prior versions; 1.1.0 version 1.1.0.1 and prior versions. **CVE ID : CVE-2021-35534**	=8DBD000059&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000058&LanguageCode=en&DocumentPartId=&Action=Launch	
Insecure Default Initialization	18-Nov-21	6.8	Insecure Boot Image vulnerability in Hitachi Energy Relion Relion	https://search.abb.com/library/Dow	O-HIT-RELI-081221/5295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Resource			670/650/SAM600-IO series allows an attacker who manages to get access to the front network port and to cause a reboot sequences of the device may exploit the vulnerability, where there is a tiny time gap during the booting process where an older version of VxWorks is loaded prior to application firmware booting, could exploit the vulnerability in the older version of VxWorks and cause a denial-of-service on the product. This issue affects: Hitachi Energy Relion 670 Series 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.3. Hitachi Energy Relion 670/650 Series 2.2.0 all revisions; 2.2.4 all revisions. Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions. **CVE ID : CVE-2021-35535**	nload.aspx?DocumentID=8DBD000061&LanguageCode=en&DocumentPartId=&Action=Launch	
relion_670_firmware					
Incorrect Authorization	18-Nov-21	9	Insufficient security control vulnerability in internal database access mechanism of Hitachi Energy Relion 670/650/SAM600-IO, Relion 650, GMS600, PWC600 allows attacker who successfully exploited this vulnerability, of which the product does not sufficiently restrict access to an internal database tables, could allow anybody with user credentials to bypass	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000059&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/l	O-HIT-RELI-081221/5296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security controls that is enforced by the product. Consequently, exploitation may lead to unauthorized modifications on data/firmware, and/or to permanently disabling the product. This issue affects: Hitachi Energy Relion 670 Series 2.0 all revisions; 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.5. Hitachi Energy Relion 670/650 Series 2.1 all revisions. 2.2.0 all revisions; 2.2.4 all revisions; Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions; 2.2.5 versions prior to 2.2.5.2. Hitachi Energy Relion 650 1.0 all revisions. 1.1 all revisions; 1.2 all revisions; 1.3 versions prior to 1.3.0.8; Hitachi Energy GMS600 1.3.0; 1.3.0.1; 1.2.0. Hitachi Energy PWC600 1.0.1 version 1.0.1.4 and prior versions; 1.1.0 version 1.1.0.1 and prior versions. **CVE ID : CVE-2021-35534**	ibrary/Download.aspx?DocumentID=8DBD000058&LanguageCode=en&DocumentPartId=&Action=Launch	
Insecure Default Initialization of Resource	18-Nov-21	6.8	Insecure Boot Image vulnerability in Hitachi Energy Relion Relion 670/650/SAM600-IO series allows an attacker who manages to get access to the front network port and to cause a reboot sequences of the device may exploit the vulnerability, where there is a tiny time gap during the	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000061&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RELI-081221/5297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			booting process where an older version of VxWorks is loaded prior to application firmware booting, could exploit the vulnerability in the older version of VxWorks and cause a denial-of-service on the product. This issue affects: Hitachi Energy Relion 670 Series 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.3. Hitachi Energy Relion 670/650 Series 2.2.0 all revisions; 2.2.4 all revisions. Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions. **CVE ID : CVE-2021-35535**		
relion_sam600-io_firmware					
Incorrect Authorization	18-Nov-21	9	Insufficient security control vulnerability in internal database access mechanism of Hitachi Energy Relion 670/650/SAM600-IO, Relion 650, GMS600, PWC600 allows attacker who successfully exploited this vulnerability, of which the product does not sufficiently restrict access to an internal database tables, could allow anybody with user credentials to bypass security controls that is enforced by the product. Consequently, exploitation may lead to unauthorized modifications on data/firmware, and/or to permanently disabling the product. This issue affects:	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000059&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000058&LanguageCode=en&DocumentPartId=&Action=	O-HIT-RELI-081221/5298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Hitachi Energy Relion 670 Series 2.0 all revisions; 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.5. Hitachi Energy Relion 670/650 Series 2.1 all revisions. 2.2.0 all revisions; 2.2.4 all revisions; Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions; 2.2.5 versions prior to 2.2.5.2. Hitachi Energy Relion 650 1.0 all revisions. 1.1 all revisions; 1.2 all revisions; 1.3 versions prior to 1.3.0.8; Hitachi Energy GMS600 1.3.0; 1.3.0.1; 1.2.0. Hitachi Energy PWC600 1.0.1 version 1.0.1.4 and prior versions; 1.1.0 version 1.1.0.1 and prior versions. **CVE ID : CVE-2021-35534**	Launch	
Insecure Default Initialization of Resource	18-Nov-21	6.8	Insecure Boot Image vulnerability in Hitachi Energy Relion Relion 670/650/SAM600-IO series allows an attacker who manages to get access to the front network port and to cause a reboot sequences of the device may exploit the vulnerability, where there is a tiny time gap during the booting process where an older version of VxWorks is loaded prior to application firmware booting, could exploit the vulnerability in the older version of VxWorks and cause a denial-of-service on the product. This issue affects:	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000061&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RELI-081221/5299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Hitachi Energy Relion 670 Series 2.2.2 all revisions; 2.2.3 versions prior to 2.2.3.3. Hitachi Energy Relion 670/650 Series 2.2.0 all revisions; 2.2.4 all revisions. Hitachi Energy Relion 670/650/SAM600-IO 2.2.1 all revisions. **CVE ID : CVE-2021-35535**		
HP					
hp-ux					
Cleartext Storage of Sensitive Information	16-Nov-21	2.1	IBM MQ 7.5, 8.0, 9.0 LTS, 9.1 CD, and 9.1 LTS stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 211403. **CVE ID : CVE-2021-38949**	https://www.ibm.com/support/pages/node/6516424	O-HP-HP-U-081221/5300
Huawei					
cloudengine_5800_firmware					
Improper Privilege Management	23-Nov-21	7.2	There is a privilege escalation vulnerability in CloudEngine 5800 V200R020C00SPC600. Due to lack of privilege restrictions, an authenticated local attacker can perform specific operation to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege. **CVE ID : CVE-2021-39976**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211103-01-privilege-en	O-HUA-CLOU-081221/5301
ecns280_td_firmware					
Exposure of Sensitive Information to an	23-Nov-21	2.1	There is an information leakage vulnerability in FusionCompute 6.5.1, eCNS280_TD V100R005C00	https://www.huawei.com/en/psirt/security-	O-HUA-ECNS-081221/5302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			and V100R005C10. Due to the improperly storage of specific information in the log file, the attacker can obtain the information when a user logs in to the device. Successful exploit may cause the information leak. **CVE ID : CVE-2021-37036**	advisories/huawei-sa-20210818-01-informationleak-en	
Out-of-bounds Read	29-Nov-21	6.8	Some Huawei products use the OpenHpi software for hardware management. A function that parses data returned by OpenHpi contains an out-of-bounds read vulnerability that could lead to a denial of service. Affected product versions include: eCNS280_TD V100R005C10; eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. **CVE ID : CVE-2021-39995**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211124-03-dos-en	O-HUA-ECNS-081221/5303
ese620x_vess_firmware					
Out-of-bounds Read	29-Nov-21	6.8	Some Huawei products use the OpenHpi software for hardware management. A function that parses data returned by OpenHpi contains an out-of-bounds read vulnerability that could lead to a denial of service. Affected product versions include: eCNS280_TD V100R005C10; eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211124-03-dos-en	O-HUA-ESE6-081221/5304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39995		
harmonyos					
Improper Input Validation	23-Nov-21	7.8	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37003**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5305
Improper Input Validation	23-Nov-21	7.8	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37004**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5306
Improper Input Validation	23-Nov-21	7.8	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37005**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5307
Improper Preservation of Permissions	23-Nov-21	5	There is a Improper Preservation of Permissions vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the confidentiality of users is	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-	O-HUA-HARM-081221/5308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected. **CVE ID : CVE-2021-37006**	202108-0000001180965965	
Out-of-bounds Read	23-Nov-21	7.8	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37007**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5309
Improper Input Validation	23-Nov-21	7.8	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37008**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5310
N/A	23-Nov-21	5	There is a Configuration vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the confidentiality of users is affected. **CVE ID : CVE-2021-37009**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5311
Exposure of Sensitive Information to an Unauthorized Actor	23-Nov-21	5	There is a Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-	O-HUA-HARM-081221/5312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			confidentiality of users is affected. **CVE ID : CVE-2021-37010**	202108-0000001180965965	
N/A	23-Nov-21	7.8	There is a Data Processing Errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37012**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5313
Improper Input Validation	23-Nov-21	5	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the availability of users is affected. **CVE ID : CVE-2021-37013**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5314
Out-of-bounds Read	23-Nov-21	7.8	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37015**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5315
Out-of-bounds Read	23-Nov-21	8.5	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause Information Disclosure or	https://device.harmonyos.com/cn/docs/security/update/security-	O-HUA-HARM-081221/5316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service. **CVE ID : CVE-2021-37016**	bulletins-202108-0000001180965965	
Improper Input Validation	23-Nov-21	7.8	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37017**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5317
N/A	23-Nov-21	7.8	There is a Data Processing Errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37018**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5318
Improper Input Validation	23-Nov-21	7.8	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37019**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5319
Out-of-bounds Write	23-Nov-21	10	There is a Heap-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause root	https://device.harmonyos.com/cn/docs/security/update/security-	O-HUA-HARM-081221/5320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permission which can be escalated. **CVE ID : CVE-2021-37022**	bulletins-202108-0000001180965965	
N/A	23-Nov-21	6.4	There is a Improper Access Control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause media files which can be reads and writes in non-distributed directories on any device on the network.. **CVE ID : CVE-2021-37023**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5321
Improper Input Validation	23-Nov-21	7.8	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37024**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5322
Improper Input Validation	23-Nov-21	7.8	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37025**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202108-0000001180965965	O-HUA-HARM-081221/5323
Improper Input Validation	23-Nov-21	7.8	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful	https://device.harmonyos.com/cn/docs/security/	O-HUA-HARM-081221/5324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability will cause kernel crash. **CVE ID : CVE-2021-37026**	update/security-bulletins-202108-0000001180965965	
imaster_nce-fabric_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	3.5	There is a XSS injection vulnerability in iMaster NCE-Fabric V100R019C10. A module of the client does not verify the input sufficiently. Attackers can exploit this vulnerability by modifying input after logging onto the client. This may compromise the normal service of the client. **CVE ID : CVE-2021-22410**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210324-01-xss-en	O-HUA-IMAS-081221/5325
ips_module_firmware					
Use of a Broken or Risky Cryptographic Algorithm	23-Nov-21	4.3	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a module. Attackers can exploit this vulnerability by capturing and analyzing the messages between devices to obtain information. This can lead to information leak.Affected product versions include: IPS Module V500R005C00SPC100, V500R005C00SPC200; NGFW Module V500R005C00SPC100, V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-infomationleak-en	O-HUA-IPS_-081221/5326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; USG9500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200. **CVE ID : CVE-2021-22356**		
ngfw_module_firmware					
Use of a Broken or Risky Cryptographic Algorithm	23-Nov-21	4.3	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a module. Attackers can exploit this vulnerability by capturing and analyzing the messages between devices to obtain information. This can lead to information leak.Affected product versions include: IPS Module V500R005C00SPC100, V500R005C00SPC200; NGFW Module V500R005C00SPC100,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-infomationleak-en	O-HUA-NGFW-081221/5327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; USG9500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200. **CVE ID : CVE-2021-22356**		
secospace_usg6300_firmware					
Use of a Broken or Risky Cryptographic Algorithm	23-Nov-21	4.3	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a module. Attackers can exploit this vulnerability by capturing and analyzing the messages between devices to obtain information. This can lead to information leak.Affected product versions include: IPS Module V500R005C00SPC100,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-infomationleak-en	O-HUA-SECO-081221/5328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00SPC200; NGFW Module V500R005C00SPC100, V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; USG9500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200. **CVE ID : CVE-2021-22356**		
secospace_usg6500_firmware					
Use of a Broken or Risky Cryptographic Algorithm	23-Nov-21	4.3	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a module. Attackers can exploit this vulnerability by capturing and analyzing the messages between devices to obtain information. This can lead to information leak.Affected	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-infomationleak-en	O-HUA-SECO-081221/5329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			product versions include: IPS Module V500R005C00SPC100, V500R005C00SPC200; NGFW Module V500R005C00SPC100, V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; USG9500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200. **CVE ID : CVE-2021-22356**		
secospace_usg6600_firmware					
Use of a Broken or Risky Cryptographic Algorithm	23-Nov-21	4.3	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a module. Attackers can exploit this vulnerability by capturing and analyzing the messages	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-	O-HUA-SECO-081221/5330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			between devices to obtain information. This can lead to information leak.Affected product versions include: IPS Module V500R005C00SPC100, V500R005C00SPC200; NGFW Module V500R005C00SPC100, V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; USG9500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200. **CVE ID : CVE-2021-22356**	01-infomationleak-en	
usg9500_firmware					
Use of a Broken or Risky Cryptographi	23-Nov-21	4.3	There is a weak secure algorithm vulnerability in Huawei products. A weak secure algorithm is used in a	https://www.huawei.com/en/psirt/security-	O-HUA-USG9-081221/5331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c Algorithm			module. Attackers can exploit this vulnerability by capturing and analyzing the messages between devices to obtain information. This can lead to information leak.Affected product versions include: IPS Module V500R005C00SPC100, V500R005C00SPC200; NGFW Module V500R005C00SPC100, V500R005C00SPC200; Secospace USG6300 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; Secospace USG6600 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200; USG9500 V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200. **CVE ID : CVE-2021-22356**	advisories/huawei-sa-20210512-01-infomationleak-en	
IBM					
aix					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	23-Nov-21	5	IBM Sterling Connect:Direct Web Services 1.0 and 6.0 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 209507. **CVE ID : CVE-2021-38890**	https://www.ibm.com/support/pages/node/6518586, https://exchange.xforce.ibmcloud.com/vulnerabilities/209507	O-IBM-AIX-081221/5332
Inadequate Encryption Strength	23-Nov-21	5	IBM Sterling Connect:Direct Web Services 1.0 and 6.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 209508. **CVE ID : CVE-2021-38891**	https://www.ibm.com/support/pages/node/6518582, https://exchange.xforce.ibmcloud.com/vulnerabilities/209508	O-IBM-AIX-081221/5333
Cleartext Storage of Sensitive Information	16-Nov-21	2.1	IBM MQ 7.5, 8.0, 9.0 LTS, 9.1 CD, and 9.1 LTS stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 211403. **CVE ID : CVE-2021-38949**	https://www.ibm.com/support/pages/node/6516424	O-IBM-AIX-081221/5334
Generation of Error Message Containing Sensitive Information	23-Nov-21	5	IBM Tivoli Key Lifecycle Manager (IBM Security Guardium Key Lifecycle Manager) 3.0, 3.0.1, 4.0, and 4.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID:	https://exchange.xforce.ibmcloud.com/vulnerabilities/212786, https://www.ibm.com/support/pages/node/6518326	O-IBM-AIX-081221/5335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212786. **CVE ID : CVE-2021-38980**		
N/A	17-Nov-21	2.1	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the libc.a library to expose sensitive information. IBM X-Force ID: 206084. **CVE ID : CVE-2021-29860**	https://www.ibm.com/support/pages/node/6516774, https://exchange.xforce.ibmcloud.com/vulnerabilities/206084	O-IBM-AIX-081221/5336
N/A	17-Nov-21	2.1	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in EFS to expose sensitive information. IBM X-Force ID: 206085. **CVE ID : CVE-2021-29861**	https://exchange.xforce.ibmcloud.com/vulnerabilities/206085, https://www.ibm.com/support/pages/node/6516786	O-IBM-AIX-081221/5337
i					
Cleartext Storage of Sensitive Information	16-Nov-21	2.1	IBM MQ 7.5, 8.0, 9.0 LTS, 9.1 CD, and 9.1 LTS stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 211403. **CVE ID : CVE-2021-38949**	https://www.ibm.com/support/pages/node/6516424	O-IBM-I-081221/5338
Intel					
7265_firmware					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an	https://www.intel.com/content/www/us/en/security-	O-INT-7265-081221/5339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	center/advisory/intel-sa-00509.html	
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-7265-081221/5340
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-7265-081221/5341
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-7265-081221/5342
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in	https://www.intel.com/content/www/us/en/security-	O-INT-7265-081221/5343

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	center/advisory/intel-sa-00509.html	
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-7265-081221/5344
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-7265-081221/5345
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-7265-081221/5346
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-7265-081221/5347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	ory/intel-sa-00509.html	
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-7265-081221/5348
9260_firmware					
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-9260-081221/5349
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-9260-081221/5350
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-9260-081221/5351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent access. **CVE ID : CVE-2021-0071**	ory/intel-sa-00509.html	
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-9260-081221/5352
ac1550_firmware					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC15-081221/5353
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC15-081221/5354
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-AC15-081221/5355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	ory/intel-sa-00509.html	
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC15-081221/5356
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC15-081221/5357
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC15-081221/5358
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-AC15-081221/5359

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2021-0082**	ory/intel-sa-00509.html	
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC15-081221/5360
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC15-081221/5361
ac_3165_firmware					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5362
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-AC_3-081221/5363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	ory/intel-sa-00509.html	
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5364
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5365
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5366
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-AC_3-081221/5367

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent access. **CVE ID : CVE-2021-0071**	ory/intel-sa-00509.html	
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5368
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5369
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5370
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-AC_3-081221/5371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0082	00509.html	
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_3-081221/5372
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_3-081221/5373
ac_3168_firmware					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5374
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-AC_3-081221/5375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via adjacent access. **CVE ID : CVE-2021-0063**	00509.html	
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5376
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5377
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5378
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-AC_3-081221/5379

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent access. **CVE ID : CVE-2021-0071**	00509.html	
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5380
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5381
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_3-081221/5382
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-AC_3-081221/5383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0082	00509.html	
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_3-081221/5384
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_3-081221/5385
ac_7265_firmware					
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_7-081221/5386
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_7-081221/5387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2021-0152**		
ac_8260_firmware					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5388
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5389
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5390
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-AC_8-081221/5391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	ory/intel-sa-00509.html	
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5392
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5393
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5394
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-AC_8-081221/5395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	00509.html	
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5396
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5397
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_8-081221/5398
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_8-081221/5399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0152		
ac_8265_firmware					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5400
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5401
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5402
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-AC_8-081221/5403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	00509.html	
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5404
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5405
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5406
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-AC_8-081221/5407

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure via adjacent access. **CVE ID : CVE-2021-0078**	00509.html	
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5408
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_8-081221/5409
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_8-081221/5410
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_8-081221/5411

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ac_9260_firmware					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5412
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5413
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5414
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5415

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0065		
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5416
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5417
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5418
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0078		
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5420
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5421
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_9-081221/5422
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_9-081221/5423
ac_9461_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5424
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5425
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5426
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5427

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5428
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5429
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5430
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5432
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5433
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_9-081221/5434
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_9-081221/5435
ac_9462_firmware					
Improper	17-Nov-21	2.7	Improper initialization in	https://ww	O-INT-AC_9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization			firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	081221/5436
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5437
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5438
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5440
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5441
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5442
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5444
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5445
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_9-081221/5446
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_9-081221/5447
ac_9560_firmware					
Improper	17-Nov-21	2.7	Improper initialization in	https://ww	O-INT-AC_9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization			firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	081221/5448
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5449
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5450
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5452
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2021-0071**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5453
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5454
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5456
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AC_9-081221/5457
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_9-081221/5458
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AC_9-081221/5459
atom_c3000_firmware					
Improper	17-Nov-21	4.6	Hardware allows activation of	https://ww	O-INT-ATOM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	081221/5460
atom_x5-e3930_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-ATOM-081221/5461
atom_x5-e3940_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-ATOM-081221/5462
atom_x7-e3950_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-ATOM-081221/5463

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ax1650_firmware					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5464
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5465
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5466
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5467

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0075		
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5468
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5469
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5470
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AX16-081221/5471
Improper	17-Nov-21	2.1	Improper verification of	https://ww	O-INT-AX16-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Verification of Cryptographic Signature			cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	081221/5472
ax1675_firmware					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5473
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0063**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5474
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0069		
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5476
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5477
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5478
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX16-081221/5479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AX16-081221/5480
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AX16-081221/5481
ax200_firmware					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5482
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0063		
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5484
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5485
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5486
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5487

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0071		
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5488
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5489
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5490
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AX20-081221/5492
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AX20-081221/5493
ax201_firmware					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5494
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0063		
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5496
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5497
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5498
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5499

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0071		
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5500
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5501
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5502
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX20-081221/5503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AX20-081221/5504
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AX20-081221/5505
ax210_firmware					
Improper Initialization	17-Nov-21	2.7	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access. **CVE ID : CVE-2021-0053**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX21-081221/5506
Improper Input Validation	17-Nov-21	6.1	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX21-081221/5507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0063		
Improper Preservation of Permissions	17-Nov-21	4.6	Insecure inherited permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0064**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX21-081221/5508
Incorrect Default Permissions	17-Nov-21	4.6	Incorrect default permissions in the Intel(R) PROSet/Wireless WiFi software installer for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0065**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX21-081221/5509
Improper Input Validation	17-Nov-21	3.3	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0069**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX21-081221/5510
Improper Input Validation	17-Nov-21	5.8	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX21-081221/5511

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0071		
Out-of-bounds Write	17-Nov-21	2.1	Out-of-bounds write in firmware for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and some Killer(TM) WiFi in Windows 10 may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0075**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX21-081221/5512
Improper Input Validation	17-Nov-21	6.8	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access. **CVE ID : CVE-2021-0078**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX21-081221/5513
Improper Input Validation	17-Nov-21	6.1	Improper input validation in software for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an unauthenticated user to potentially enable denial of service via adjacent access. **CVE ID : CVE-2021-0079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX21-081221/5514
Uncontrolled Search Path Element	17-Nov-21	4.4	Uncontrolled search path in software installer for Intel(R) PROSet/Wireless WiFi in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0082**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html	O-INT-AX21-081221/5515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0151**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AX21-081221/5516
Improper Verification of Cryptographic Signature	17-Nov-21	2.1	Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html	O-INT-AX21-081221/5517
celeron_j1750_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5518
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5519
celeron_j1800_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5520
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5521
celeron_j1850_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5522
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5523
celeron_j1900_firmware					
Improper Privilege	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime	https://www.intel.com/	O-INT-CELE-081221/5524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	content/www/us/en/security-center/advisory/intel-sa-00528.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5525
celeron_j3060_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5526
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5527
celeron_j3160_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an	https://www.intel.com/content/www/us/en/se	O-INT-CELE-081221/5528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	curity-center/advisory/intel-sa-00528.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5529
celeron_j3355e_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5530
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5531
celeron_j3355_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-CELE-081221/5532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via physical access. **CVE ID : CVE-2021-0146**	ory/intel-sa-00528.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5533
celeron_j3455e_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5534
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5535
celeron_j3455_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0146		
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5537
celeron_j4005_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5538
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5539
celeron_j4025_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5541
celeron_j4105_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5542
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5543
celeron_j4125_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5544
Improper Input	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK	https://www.intel.com/	O-INT-CELE-081221/5545

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	content/www/us/en/security-center/advisory/intel-sa-00548.html	
celeron_j6412_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5546
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5547
celeron_j6413_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5548
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may	https://www.intel.com/content/www/us/en/se	O-INT-CELE-081221/5549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	curity-center/advisory/intel-sa-00548.html	
celeron_n2805_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5550
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5551
celeron_n2806_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5552
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-CELE-081221/5553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	ory/intel-sa-00548.html	
celeron_n2807_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5554
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5555
celeron_n2808_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5556
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0186		
celeron_n2810_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5558
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5559
celeron_n2815_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5560
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
celeron_n2820_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5562
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5563
celeron_n2830_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5564
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5565
celeron_n2840_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5566
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5567
celeron_n2910_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5568
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5569
celeron_n2920_firmware					
Improper Privilege	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime	https://www.intel.com/	O-INT-CELE-081221/5570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	content/www/us/en/security-center/advisory/intel-sa-00528.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5571
celeron_n2930_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5572
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5573
celeron_n2940_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an	https://www.intel.com/content/www/us/en/se	O-INT-CELE-081221/5574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	curity-center/advisory/intel-sa-00528.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5575
celeron_n3000_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5576
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5577
celeron_n3010_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-CELE-081221/5578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege via physical access. **CVE ID : CVE-2021-0146**	ory/intel-sa-00528.html	
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5579
celeron_n3050_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5580
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5581
celeron_n3060_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0146		
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5583
celeron_n3150_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5584
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5585
celeron_n3160_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5587
celeron_n3350e_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5588
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5589
celeron_n3350_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5590
Improper Input	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK	https://www.intel.com/	O-INT-CELE-081221/5591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	content/www/us/en/security-center/advisory/intel-sa-00548.html	
celeron_n3450_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5592
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5593
celeron_n4000_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5594
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may	https://www.intel.com/content/www/us/en/se	O-INT-CELE-081221/5595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	curity-center/advisory/intel-sa-00548.html	
celeron_n4020_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5596
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5597
celeron_n4100_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5598
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-CELE-081221/5599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	ory/intel-sa-00548.html	
celeron_n4120_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5600
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5601
celeron_n4500_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5602
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0186		
celeron_n4505_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5604
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5605
celeron_n5100_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5606
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
celeron_n5105_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5608
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5609
celeron_n6210_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5610
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5611
celeron_n6211_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-CELE-081221/5612
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CELE-081221/5613
core_i3-1000g1_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5614
core_i3-1000g4_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5615
core_i3-1005g1_firmware					
Improper Input	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK	https://www.intel.com/	O-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	content/www/us/en/security-center/advisory/intel-sa-00548.html	081221/5616
core_i3-10100e_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5617
core_i3-10100f_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5618
core_i3-10100te_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5619
core_i3-10100t_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for	https://www.intel.com/content/ww	O-INT-CORE-081221/5620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w/us/en/security-center/advisory/intel-sa-00548.html	
core_i3-10100y_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5621
core_i3-10100_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5622
core_i3-10105f_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5623
core_i3-10105t_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may	https://www.intel.com/content/www/us/en/se	O-INT-CORE-081221/5624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	curity-center/advisory/intel-sa-00548.html	
core_i3-10105_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5625
core_i3-10110u_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5626
core_i3-10110y_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5627
core_i3-10300t_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to	https://www.intel.com/content/www/us/en/security-	O-INT-CORE-081221/5628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	center/advisory/intel-sa-00548.html	
core_i3-10300_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5629
core_i3-10305t_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5630
core_i3-10305_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5631
core_i3-10320_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-CORE-081221/5632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	ory/intel-sa-00548.html	
core_i3-10325_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5633
core_i5-10200h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5634
core_i5-10210u_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5635
core_i5-10210y_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-CORE-081221/5636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0186	00548.html	
core_i5-10300h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5637
core_i5-1030g4_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5638
core_i5-1030g7_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5639
core_i5-10310u_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i5-10310y_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5641
core_i5-1035g1_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5642
core_i5-1035g4_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5643
core_i5-1035g7_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5644
core_i5-1038ng7_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5645
core_i5-10400f_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5646
core_i5-10400h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5647
core_i5-10400t_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5648
core_i5-10400_firmware					
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	O-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	081221/5649
core_i5-10500e_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5650
core_i5-10500h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5651
core_i5-10500te_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5652
core_i5-10500t_firmware					
Improper Input	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK	https://www.intel.com/	O-INT-CORE-081221/5653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	content/www/us/en/security-center/advisory/intel-sa-00548.html	
core_i5-10500_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5654
core_i5-10505_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5655
core_i5-10600kf_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5656
core_i5-10600k_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for	https://www.intel.com/content/ww	O-INT-CORE-081221/5657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w/us/en/security-center/advisory/intel-sa-00548.html	
core_i5-10600t_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5658
core_i5-10600_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5659
core_i7-10510u_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5660
core_i7-10510y_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may	https://www.intel.com/content/www/us/en/se	O-INT-CORE-081221/5661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	curity-center/advisory/intel-sa-00548.html	
core_i7-1060g7_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5662
core_i7-10610u_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5663
core_i7-1065g7_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5664
core_i7-1068ng7_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to	https://www.intel.com/content/www/us/en/security-	O-INT-CORE-081221/5665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	center/advisory/intel-sa-00548.html	
core_i7-10700e_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5666
core_i7-10700f_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5667
core_i7-10700kf_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5668
core_i7-10700k_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-CORE-081221/5669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	ory/intel-sa-00548.html	
core_i7-10700te_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5670
core_i7-10700t_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5671
core_i7-10700_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5672
core_i7-10710u_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-CORE-081221/5673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0186	00548.html	
core_i7-10750h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5674
core_i7-10810u_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5675
core_i7-10850h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5676
core_i7-10870h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
core_i7-10875h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5678
core_i9-10850k_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5679
core_i9-10885h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5680
core_i9-10900e_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5681
core_i9-10900f_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5682
core_i9-10900kf_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5683
core_i9-10900k_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5684
core_i9-10900te_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5685
core_i9-10900t_firmware					
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	O-INT-CORE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	081221/5686
core_i9-10900_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5687
core_i9-10980hk_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-CORE-081221/5688
ethernet_controller_v710-at2_firmware					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5689
ethernet_controller_x710-am2_firmware					
Out-of-	17-Nov-21	4.6	Out-of-bounds write in the	https://ww	O-INT-ETHE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	081221/5690
ethernet_controller_x710-at2_firmware					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5691
ethernet_controller_x710-bm2_firmware					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5692
ethernet_controller_x710-tm4_firmware					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5693

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ethernet_controller_xl710-am1_firmware					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5694
ethernet_controller_xl710-am2_firmware					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5695
ethernet_controller_xl710-bm1_firmware					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5696
ethernet_controller_xl710-bm2_firmware					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-ETHE-081221/5697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2021-0200**	00554.html	
ethernet_controller_xxv710-am1_firmware					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5698
ethernet_controller_xxv710-am2_firmware					
Out-of-bounds Write	17-Nov-21	4.6	Out-of-bounds write in the firmware for Intel(R) Ethernet 700 Series Controllers before version 8.2 may allow a privileged user to potentially enable an escalation of privilege via local access. **CVE ID : CVE-2021-0200**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5699
ethernet_network_controller_e810-cam1_firmware					
N/A	17-Nov-21	2.1	Protection mechanism failure in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to enable a denial of service via local access. **CVE ID : CVE-2021-0197**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5700
Incorrect Authorization	17-Nov-21	2.1	Improper access control in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to potentially enable a denial of	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-ETHE-081221/5701

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2021-0198**	ory/intel-sa-00554.html	
Improper Input Validation	17-Nov-21	2.1	Improper input validation in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.6.0.6 may allow a privileged user to potentially enable a denial of service via local access. **CVE ID : CVE-2021-0199**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5702
ethernet_network_controller_e810-cam2_firmware					
N/A	17-Nov-21	2.1	Protection mechanism failure in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to enable a denial of service via local access. **CVE ID : CVE-2021-0197**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5703
Incorrect Authorization	17-Nov-21	2.1	Improper access control in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to potentially enable a denial of service via local access. **CVE ID : CVE-2021-0198**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5704
Improper Input Validation	17-Nov-21	2.1	Improper input validation in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.6.0.6 may allow a privileged user to potentially enable a denial of service via local access. **CVE ID : CVE-2021-0199**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5705
ethernet_network_controller_e810-xxvam2_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Nov-21	2.1	Protection mechanism failure in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to enable a denial of service via local access. **CVE ID : CVE-2021-0197**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5706
Incorrect Authorization	17-Nov-21	2.1	Improper access control in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.5.5.6 may allow a privileged user to potentially enable a denial of service via local access. **CVE ID : CVE-2021-0198**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5707
Improper Input Validation	17-Nov-21	2.1	Improper input validation in the firmware for the Intel(R) Ethernet Network Controller E810 before version 1.6.0.6 may allow a privileged user to potentially enable a denial of service via local access. **CVE ID : CVE-2021-0199**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00554.html	O-INT-ETHE-081221/5708
nuc7i3dn_firmware					
Improper Authentication	17-Nov-21	4.6	Improper authentication in the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC7i3DN, NUC7i5DN, NUC7i7DN before version 1.78.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0096**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	O-INT-NUC7-081221/5709
nuc7i5dn_firmware					
Improper	17-Nov-21	4.6	Improper authentication in	https://ww	O-INT-NUC7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC7i3DN, NUC7i5DN, NUC7i7DN before version 1.78.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0096**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	081221/5710
nuc7i7dn_firmware					
Improper Authentication	17-Nov-21	4.6	Improper authentication in the software installer for the Intel(R) NUC HDMI Firmware Update Tool for NUC7i3DN, NUC7i5DN, NUC7i7DN before version 1.78.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0096**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00568.html	O-INT-NUC7-081221/5711
nuc_10_performance_kit_nuc10i3fnhfa_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5712
nuc_10_performance_kit_nuc10i3fnhf_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nuc_10_performance_kit_nuc10i3fnhja_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5714
nuc_10_performance_kit_nuc10i3fnh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5715
nuc_10_performance_kit_nuc10i3fnk_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5716
nuc_10_performance_kit_nuc10i5fnhca_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5717
nuc_10_performance_kit_nuc10i5fnhf_firmware					
Out-of-	17-Nov-21	4.9	Out-of-bounds write in	https://ww	O-INT-NUC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	081221/5718
nuc_10_performance_kit_nuc10i5fnhja_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5719
nuc_10_performance_kit_nuc10i5fnhj_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5720
nuc_10_performance_kit_nuc10i5fnh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5721
nuc_10_performance_kit_nuc10i5fnkpa_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an	https://www.intel.com/content/ww	O-INT-NUC_-081221/5722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w/us/en/security-center/advisory/intel-sa-00567.html	
nuc_10_performance_kit_nuc10i5fnkp_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5723
nuc_10_performance_kit_nuc10i5fnk_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5724
nuc_10_performance_kit_nuc10i7fnhaa_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5725
nuc_10_performance_kit_nuc10i7fnhc_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-	O-INT-NUC_-081221/5726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2021-33086**	center/advisory/intel-sa-00567.html	
nuc_10_performance_kit_nuc10i7fnhja_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5727
nuc_10_performance_kit_nuc10i7fnh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5728
nuc_10_performance_kit_nuc10i7fnkpa_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5729
nuc_10_performance_kit_nuc10i7fnkp_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-NUC_-081221/5730

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00567.html	
nuc_10_performance_kit_nuc10i7fnk_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5731
nuc_11_compute_element_cm11ebc4w_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5732
nuc_11_compute_element_cm11ebi38w_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5733
nuc_11_compute_element_cm11ebi58w_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5734
nuc_11_compute_element_cm11ebi716w_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5735
nuc_11_enthusiast_kit_nuc11phki7c_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5736
nuc_11_enthusiast_mini_pc_nuc11phki7caa_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5737
nuc_11_performance_kit_nuc11pahi3_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5738
nuc_11_performance_kit_nuc11pahi5_firmware					
Out-of-bounds	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R)	https://www.intel.com/	O-INT-NUC_-081221/5739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	content/www/us/en/security-center/advisory/intel-sa-00567.html	
nuc_11_performance_kit_nuc11pahi7_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5740
nuc_11_performance_kit_nuc11paki3_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5741
nuc_11_performance_kit_nuc11paki5_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5742
nuc_11_performance_kit_nuc11paki7_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to	https://www.intel.com/content/www/us/en/se	O-INT-NUC_-081221/5743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	curity-center/advisory/intel-sa-00567.html	
nuc_11_performance_mini_pc_nuc11paqi50wa_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5744
nuc_11_performance_mini_pc_nuc11paqi70qa_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5745
nuc_11_pro_board_nuc11tnbi3_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5746
nuc_11_pro_board_nuc11tnbi5_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access.	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-NUC_-081221/5747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-33086	ory/intel-sa-00567.html	
nuc_11_pro_board_nuc11tnbi7_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5748
nuc_11_pro_kit_nuc11tnhi30l_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5749
nuc_11_pro_kit_nuc11tnhi30p_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5750
nuc_11_pro_kit_nuc11tnhi3_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nuc_11_pro_kit_nuc11tnhi50l_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5752
nuc_11_pro_kit_nuc11tnhi50w_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5753
nuc_11_pro_kit_nuc11tnhi5_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5754
nuc_11_pro_kit_nuc11tnhi70l_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5755
nuc_11_pro_kit_nuc11tnhi70q_firmware					
Out-of-	17-Nov-21	4.9	Out-of-bounds write in	https://ww	O-INT-NUC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	081221/5756
nuc_11_pro_kit_nuc11tnhi7_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5757
nuc_11_pro_kit_nuc11tnki3_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5758
nuc_11_pro_kit_nuc11tnki5_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5759
nuc_11_pro_kit_nuc11tnki7_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an	https://www.intel.com/content/ww	O-INT-NUC_-081221/5760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w/us/en/security-center/advisory/intel-sa-00567.html	
nuc_7_business_nuc7i3dnhnc_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5761
nuc_7_business_nuc7i3dnktc_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5762
nuc_7_business_nuc7i5dnbe_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5763
nuc_7_business_nuc7i5dnhe_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-	O-INT-NUC_-081221/5764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2021-33086**	center/advisory/intel-sa-00567.html	
nuc_7_business_nuc7i5dnke_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5765
nuc_7_business_nuc7i5dnkpc_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5766
nuc_7_essential_nuc7cjysal_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5767
nuc_8_business_nuc8i7hnkqc_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-NUC_-081221/5768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00567.html	
nuc_8_compute_element_cm8ccb_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5769
nuc_8_compute_element_cm8i3cb_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5770
nuc_8_compute_element_cm8i5cb_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5771
nuc_8_compute_element_cm8i7cb_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5772
nuc_8_compute_element_cm8pcb_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5773
nuc_8_enthusiast_nuc8i7behga_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5774
nuc_8_enthusiast_nuc8i7bekqa_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5775
nuc_8_enthusiast_nuc8i7hvkvaw_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5776
nuc_8_enthusiast_nuc8i7hvkva_firmware					
Out-of-bounds	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R)	https://www.intel.com/	O-INT-NUC_-081221/5777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	content/www/us/en/security-center/advisory/intel-sa-00567.html	
nuc_8_home_nuc8i3behfa_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5778
nuc_8_home_nuc8i3cysm_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5779
nuc_8_home_nuc8i3cysn_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5780
nuc_8_home_nuc8i5behfa_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to	https://www.intel.com/content/www/us/en/se	O-INT-NUC_-081221/5781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	curity-center/advisory/intel-sa-00567.html	
nuc_8_home_nuc8i5bekpa_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5782
nuc_8_mainstream-g_kit_nuc8i5inh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5783
nuc_8_mainstream-g_kit_nuc8i7inh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5784
nuc_8_mainstream-g_mini_pc_nuc8i5inh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access.	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-NUC_-081221/5785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-33086	ory/intel-sa-00567.html	
nuc_8_mainstream-g_mini_pc_nuc8i7inh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5786
nuc_8_pro_board_nuc8i3pnb_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5787
nuc_8_pro_kit_nuc8i3pnh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5788
nuc_8_pro_kit_nuc8i3pnk_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nuc_8_rugged_kit_nuc8cchkr_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5790
nuc_9_pro_compute_element_nuc9v7qnb_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5791
nuc_9_pro_compute_element_nuc9vxqnb_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5792
nuc_9_pro_kit_nuc9v7qnx_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5793
nuc_9_pro_kit_nuc9vxqnx_firmware					
Out-of-	17-Nov-21	4.9	Out-of-bounds write in	https://ww	O-INT-NUC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	081221/5794
nuc_board_nuc7i3dnbe_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5795
nuc_board_nuc8cchb_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5796
nuc_kit_nuc6cayh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5797
nuc_kit_nuc6cays_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an	https://www.intel.com/content/www	O-INT-NUC_-081221/5798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	w/us/en/security-center/advisory/intel-sa-00567.html	
nuc_kit_nuc7cjyh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5799
nuc_kit_nuc7i3dnhe_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5800
nuc_kit_nuc7i3dnke_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5801
nuc_kit_nuc7pjyh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-	O-INT-NUC_-081221/5802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2021-33086**	center/advisory/intel-sa-00567.html	
nuc_kit_nuc8i3behs_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5803
nuc_kit_nuc8i3beh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5804
nuc_kit_nuc8i3bek_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5805
nuc_kit_nuc8i5behs_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-NUC_-081221/5806

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00567.html	
nuc_kit_nuc8i5beh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5807
nuc_kit_nuc8i5bek_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5808
nuc_kit_nuc8i7beh_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5809
nuc_kit_nuc8i7bek_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5810
nuc_kit_nuc8i7hnk_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5811
nuc_kit_nuc8i7hvk_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5812
nuc_m15_laptop_kit_audio_driver_pack					
Incorrect Permission Assignment for Critical Resource	17-Nov-21	7.2	Insecure inherited permissions in the installer for the Intel(R) NUC M15 Laptop Kit audio driver pack before version 1.3 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33091**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	O-INT-NUC_-081221/5813
nuc_m15_laptop_kit_hid_event_filter_driver_pack					
Incorrect Default Permissions	17-Nov-21	7.2	Incorrect default permissions in the installer for the Intel(R) NUC M15 Laptop Kit HID Event Filter driver pack before version 2.2.1.383 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33092**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	O-INT-NUC_-081221/5814
nuc_m15_laptop_kit_integrated_sensor_hub_driver_pack					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	17-Nov-21	7.2	Incorrect default permissions in the installer for the Intel(R) NUC M15 Laptop Kit Integrated Sensor Hub driver pack before version 5.4.1.4449 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33088**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	O-INT-NUC_-081221/5815
nuc_m15_laptop_kit_keyboard_led_service_driver_pack					
Incorrect Permission Assignment for Critical Resource	17-Nov-21	7.2	Insecure inherited permissions in the installer for the Intel(R) NUC M15 Laptop Kit Keyboard LED Service driver pack before version 1.0.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33094**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	O-INT-NUC_-081221/5816
Unquoted Search Path or Element	17-Nov-21	7.2	Unquoted search path in the installer for the Intel(R) NUC M15 Laptop Kit Keyboard LED Service driver pack before version 1.0.0.4 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33095**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	O-INT-NUC_-081221/5817
nuc_m15_laptop_kit_lapbc510_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-NUC_-081221/5818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00567.html	
nuc_m15_laptop_kit_lapbc710_firmware					
Out-of-bounds Write	17-Nov-21	4.9	Out-of-bounds write in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33086**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00567.html	O-INT-NUC_-081221/5819
nuc_m15_laptop_kit_management_engine_driver_pack					
Improper Authentication	17-Nov-21	4.9	Improper authentication in the installer for the Intel(R) NUC M15 Laptop Kit Management Engine driver pack before version 15.0.10.1508 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-33087**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	O-INT-NUC_-081221/5820
nuc_m15_laptop_kit_serial_io_driver_pack					
Incorrect Permission Assignment for Critical Resource	17-Nov-21	7.2	Insecure inherited permissions in the installer for the Intel(R) NUC M15 Laptop Kit Serial IO driver pack before version 30.100.2104.1 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33093**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00569.html	O-INT-NUC_-081221/5821
pentium_j2850_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to	https://www.intel.com/content/www/us/en/security-	O-INT-PENT-081221/5822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	center/advisory/intel-sa-00528.html	
pentium_j2900_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5823
pentium_j3710_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5824
pentium_j4205_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5825
pentium_j6426_firmware					
Improper Privilege	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime	https://www.intel.com/	O-INT-PENT-081221/5826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	content/www/us/en/security-center/advisory/intel-sa-00528.html	
pentium_n3510_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5827
pentium_n3520_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5828
pentium_n3530_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pentium_n3540_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5830
pentium_n3700_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5831
pentium_n3710_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5832
pentium_n4200e_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-PENT-081221/5833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access. **CVE ID : CVE-2021-0146**	00528.html	
pentium_n4200_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5834
pentium_n6415_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5835
pentium_silver_j5005_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5836
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-PENT-081221/5837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	ory/intel-sa-00548.html	
pentium_silver_j5040_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5838
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-PENT-081221/5839
pentium_silver_n5000_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5840
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-PENT-081221/5841

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0186		
pentium_silver_n5030_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5842
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-PENT-081221/5843
pentium_silver_n6000_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5844
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-PENT-081221/5845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pentium_silver_n6005_firmware					
Improper Privilege Management	17-Nov-21	4.6	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2021-0146**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html	O-INT-PENT-081221/5846
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-PENT-081221/5847
ssd_d-s4510_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5848
ssd_d5-p4320_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5849
ssd_d5-p4326_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5850
ssd_d5-p4420_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5851
ssd_d7-p5500_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5852
ssd_d7-p5600_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5853
ssd_d7-p5608_firmware					
Insertion of Sensitive	17-Nov-21	2.1	Insertion of information into log file in firmware for some	https://www.intel.com/	O-INT-SSD_-081221/5854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information into Log File			Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	content/www/us/en/security-center/advisory/intel-sa-00535.html	
ssd_dc_d4512_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5855
ssd_dc_p4500_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5856
ssd_dc_p4501_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5857
ssd_dc_p4510_edsff_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially	https://www.intel.com/content/www/us/en/se	O-INT-SSD_-081221/5858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable information disclosure via local access. **CVE ID : CVE-2021-0148**	curity-center/advisory/intel-sa-00535.html	
ssd_dc_p4510_u.2_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5859
ssd_dc_p4511_edsff_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5860
ssd_dc_p4511_m.2_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5861
ssd_dc_p4600_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access.	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-SSD_-081221/5862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0148	ory/intel-sa-00535.html	
ssd_dc_p4608_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5863
ssd_dc_p4610_u.2_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5864
ssd_dc_p4618_firmware					
Insertion of Sensitive Information into Log File	17-Nov-21	2.1	Insertion of information into log file in firmware for some Intel(R) SSD DC may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2021-0148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00535.html	O-INT-SSD_-081221/5865
xeon_gold_5315y_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xeon_gold_5317_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5867
xeon_gold_5318h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5868
xeon_gold_5318n_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5869
xeon_gold_5318s_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5870
xeon_gold_5318y_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5871
xeon_gold_5320h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5872
xeon_gold_5320t_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5873
xeon_gold_5320_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5874
xeon_gold_6312u_firmware					
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	O-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	081221/5875
xeon_gold_6314u_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5876
xeon_gold_6326_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5877
xeon_gold_6328hl_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5878
xeon_gold_6328h_firmware					
Improper Input	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK	https://www.intel.com/	O-INT-XEON-081221/5879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	content/www/us/en/security-center/advisory/intel-sa-00548.html	
xeon_gold_6330h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5880
xeon_gold_6330n_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5881
xeon_gold_6330_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5882
xeon_gold_6334_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for	https://www.intel.com/content/ww	O-INT-XEON-081221/5883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w/us/en/security-center/advisory/intel-sa-00548.html	
xeon_gold_6336y_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5884
xeon_gold_6338n_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5885
xeon_gold_6338t_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5886
xeon_gold_6338_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may	https://www.intel.com/content/www/us/en/se	O-INT-XEON-081221/5887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	curity-center/advisory/intel-sa-00548.html	
xeon_gold_6342_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5888
xeon_gold_6346_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5889
xeon_gold_6348h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5890
xeon_gold_6348_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to	https://www.intel.com/content/www/us/en/security-	O-INT-XEON-081221/5891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	center/advisory/intel-sa-00548.html	
xeon_gold_6354_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5892
xeon_platinum_8351n_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5893
xeon_platinum_8352m_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5894
xeon_platinum_8352s_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of	https://www.intel.com/content/www/us/en/security-center/advis	O-INT-XEON-081221/5895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2021-0186**	ory/intel-sa-00548.html	
xeon_platinum_8352v_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5896
xeon_platinum_8352y_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5897
xeon_platinum_8353h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5898
xeon_platinum_8354h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-XEON-081221/5899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0186	00548.html	
xeon_platinum_8356h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5900
xeon_platinum_8358p_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5901
xeon_platinum_8358_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5902
xeon_platinum_8360hl_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xeon_platinum_8360h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5904
xeon_platinum_8360y_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5905
xeon_platinum_8362_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5906
xeon_platinum_8368q_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5907
xeon_platinum_8368_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5908
xeon_platinum_8376hl_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5909
xeon_platinum_8376h_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5910
xeon_platinum_8380hl_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5911
xeon_platinum_8380h_firmware					
Improper	17-Nov-21	4.6	Improper input validation in	https://ww	O-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	w.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	081221/5912
xeon_platinum_8380_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5913
xeon_silver_4309y_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5914
xeon_silver_4310t_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5915
xeon_silver_4310_firmware					
Improper Input	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK	https://www.intel.com/	O-INT-XEON-081221/5916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	content/www/us/en/security-center/advisory/intel-sa-00548.html	
xeon_silver_4314_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5917
xeon_silver_4316_firmware					
Improper Input Validation	17-Nov-21	4.6	Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access. **CVE ID : CVE-2021-0186**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html	O-INT-XEON-081221/5918
iptime					
c200_firmware					
N/A	22-Nov-21	10	ius_get.cgi in IpTime C200 camera allows remote code execution. A remote attacker may send a crafted parameters to the exposed vulnerable web service interface which invokes the arbitrary shell command. **CVE ID : CVE-2021-26614**	N/A	O-IPT-C200-081221/5919
Linux					
linux_kernel					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-LIN-LINU-081221/5920
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-LIN-LINU-081221/5921
N/A	16-Nov-21	2.1	IBM Spectrum Scale 5.1.0 through 5.1.1.1 could allow a privileged admin to destroy filesystem audit logging records before expiration time. IBM X-Force ID: 209164. **CVE ID : CVE-2021-38882**	https://www.ibm.com/support/pages/node/6516426	O-LIN-LINU-081221/5922
Improper Restriction of Excessive Authentication Attempts	23-Nov-21	5	IBM Sterling Connect:Direct Web Services 1.0 and 6.0 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 209507. **CVE ID : CVE-2021-38890**	https://www.ibm.com/support/pages/node/6518586, https://exchange.xforce.ibmcloud.com/vulnerabilities/209507	O-LIN-LINU-081221/5923
Inadequate	23-Nov-21	5	IBM Sterling Connect:Direct	https://ww	O-LIN-LINU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Encryption Strength			Web Services 1.0 and 6.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 209508. **CVE ID : CVE-2021-38891**	w.ibm.com/support/pages/node/6518582, https://exchange.xforce.ibmcloud.com/vulnerabilities/209508	081221/5924
Cleartext Storage of Sensitive Information	16-Nov-21	2.1	IBM MQ 7.5, 8.0, 9.0 LTS, 9.1 CD, and 9.1 LTS stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 211403. **CVE ID : CVE-2021-38949**	https://www.ibm.com/support/pages/node/6516424	O-LIN-LINU-081221/5925
Generation of Error Message Containing Sensitive Information	23-Nov-21	5	IBM Tivoli Key Lifecycle Manager (IBM Security Guardium Key Lifecycle Manager) 3.0, 3.0.1, 4.0, and 4.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 212786. **CVE ID : CVE-2021-38980**	https://exchange.xforce.ibmcloud.com/vulnerabilities/212786, https://www.ibm.com/support/pages/node/6518326	O-LIN-LINU-081221/5926
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Nov-21	5	Adobe Campaign version 21.2.1 (and earlier) is affected by a Path Traversal vulnerability that could lead to reading arbitrary server files. By leveraging an exposed XML file, an unauthenticated attacker can enumerate other files on the	https://helpx.adobe.com/security/products/campaign/apsb21-52.html	O-LIN-LINU-081221/5927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server. **CVE ID : CVE-2021-40745**		
Out-of-bounds Write	17-Nov-21	4.6	In the Linux kernel through 5.15.2, hw_atl_utils_fw_rpc_wait in drivers/net/ethernet/aquantia/atlantic/hw_atl/hw_atl_utils.c allows an attacker (who can introduce a crafted device) to trigger an out-of-bounds write via a crafted length value. **CVE ID : CVE-2021-43975**	https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=b922f622592af76b57cbc566eaeccda0b31a3496, https://lore.kernel.org/netdev/163698540868.13805.1780040802178240876 2.git-patchwork-notify@kernel.org/T/	O-LIN-LINU-081221/5928
N/A	17-Nov-21	2.1	In the Linux kernel through 5.15.2, mwifiex_usb_recv in drivers/net/wireless/marvell/mwifiex/usb.c allows an attacker (who can connect a crafted USB device) to cause a denial of service (skb_over_panic). **CVE ID : CVE-2021-43976**	https://patchwork.kernel.org/project/linux-wireless/patch/YX4CqjfRcTa6bVL+@Zekuns-MBP-16.fios-router.home/	O-LIN-LINU-081221/5929
Improper Neutralization of Input During Web Page Generation	29-Nov-21	3.5	Self cross-site scripting (XSS) was possible on devices page. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux)	https://security-advisory.acronis.com/advisories/SEC	O-LIN-LINU-081221/5930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			before build 28035 **CVE ID : CVE-2021-44200**	-2803	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	4.3	Cross-site scripting (XSS) was possible in notification pop-ups. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035 **CVE ID : CVE-2021-44201**	https://security-advisory.acronis.com/advisories/SEC-3167	O-LIN-LINU-081221/5931
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	Stored cross-site scripting (XSS) was possible in activity details. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035 **CVE ID : CVE-2021-44202**	https://security-advisory.acronis.com/advisories/SEC-3283	O-LIN-LINU-081221/5932
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	Stored cross-site scripting (XSS) was possible in protection plan details. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035 **CVE ID : CVE-2021-44203**	https://security-advisory.acronis.com/advisories/SEC-3294	O-LIN-LINU-081221/5933
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-LIN-LINU-081221/5934
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra	https://nvid	O-LIN-LINU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	ia.custhelp.com/app/answers/detail/a_id/5263	081221/5935
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-LIN-LINU-081221/5936
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-LIN-LINU-081221/5937
Integer Overflow or Wraparound	26-Nov-21	6.8	ARK library allows attackers to execute remote code via the parameter(path value) of Ark_NormalizeAndDupPAthNameW function because of an integer overflow. **CVE ID : CVE-2021-26615**	N/A	O-LIN-LINU-081221/5938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-LIN-LINU-081221/5939
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-LIN-LINU-081221/5940
Incorrect Default Permissions	24-Nov-21	4.6	When Octopus Tentacle is installed on a Linux operating system, the systemd service file permissions are misconfigured. This could lead to a local unprivileged user modifying the contents of the systemd service file to gain privileged access. **CVE ID : CVE-2021-31822**	https://advisories.octopus.com/adv/2021-11---Local-privilege-escalation-in-Octopus-Tentacle-(CVE-2021-31822).2283732993.html	O-LIN-LINU-081221/5941
micron					
ddr4_sdram_firmware					
N/A	16-Nov-21	7.9	Modern DRAM devices (PC-DDR4, LPDDR4X) are affected by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer	https://comsec.ethz.ch/wp-content/files/blacksmith_sp22.pdf	O-MIC-DDR4-081221/5942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access patterns, consisting of aggressors with different frequencies, phases, and amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example, this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three major DRAM vendors (Samsung, SK Hynix, Micron) are affected by this vulnerability. For more details, please refer to our publication. **CVE ID : CVE-2021-42114**		
lddr4_firmware					
N/A	16-Nov-21	7.9	Modern DRAM devices (PC-DDR4, LPDDR4X) are affected	https://comsec.ethz.ch/	O-MIC-LDDR-081221/5943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer access patterns, consisting of aggressors with different frequencies, phases, and amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example, this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three major DRAM vendors (Samsung, SK Hynix, Micron) are affected by this vulnerability. For more details, please refer to our publication.	wp-content/files/blacksmith_sp22.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-42114		
Microsoft					
windows					
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed registers, which may lead to information disclosure. **CVE ID : CVE-2021-34399**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-MIC-WIND-081221/5944
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to gain access to information from unscrubbed memory, which may lead to information disclosure. **CVE ID : CVE-2021-34400**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-MIC-WIND-081221/5945
Out-of-bounds Read	19-Nov-21	4.3	Adobe Audition version 14.2 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose arbitrary memory information 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-2021-36003**	https://helpx.adobe.com/security/products/audition/apsb21-62.html	O-MIC-WIND-081221/5946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	23-Nov-21	5	IBM Sterling Connect:Direct Web Services 1.0 and 6.0 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 209507. **CVE ID : CVE-2021-38890**	https://www.ibm.com/support/pages/node/6518586, https://exchange.xforce.ibmcloud.com/vulnerabilities/209507	O-MIC-WIND-081221/5947
Inadequate Encryption Strength	23-Nov-21	5	IBM Sterling Connect:Direct Web Services 1.0 and 6.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 209508. **CVE ID : CVE-2021-38891**	https://www.ibm.com/support/pages/node/6518582, https://exchange.xforce.ibmcloud.com/vulnerabilities/209508	O-MIC-WIND-081221/5948
Cleartext Storage of Sensitive Information	16-Nov-21	2.1	IBM MQ 7.5, 8.0, 9.0 LTS, 9.1 CD, and 9.1 LTS stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 211403. **CVE ID : CVE-2021-38949**	https://www.ibm.com/support/pages/node/6516424	O-MIC-WIND-081221/5949
Out-of-bounds Write	17-Nov-21	2.1	IBM SPSS Statistics for Windows 24.0, 25.0, 26.0, 27.0, 27.0.1, and 28.0 could allow a local user to cause a denial of service by writing arbitrary files to admin protected directories on the system. IBM X-Force ID: 212046. **CVE ID : CVE-2021-38959**	https://exchange.xforce.ibmcloud.com/vulnerabilities/212046, https://www.ibm.com/support/pages/node/6516680	O-MIC-WIND-081221/5950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	23-Nov-21	5	IBM Tivoli Key Lifecycle Manager (IBM Security Guardium Key Lifecycle Manager) 3.0, 3.0.1, 4.0, and 4.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 212786. **CVE ID : CVE-2021-38980**	https://exchange.xforce.ibmcloud.com/vulnerabilities/212786, https://www.ibm.com/support/pages/node/6518326	O-MIC-WIND-081221/5951
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe Animate version 21.0.9 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious .psd file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. **CVE ID : CVE-2021-40733**	https://helpx.adobe.com/security/products/animate/apsb21-105.html	O-MIC-WIND-081221/5952
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Nov-21	5	Adobe Campaign version 21.2.1 (and earlier) is affected by a Path Traversal vulnerability that could lead to reading arbitrary server files. By leveraging an exposed XML file, an unauthenticated attacker can enumerate other files on the server. **CVE ID : CVE-2021-40745**	https://helpx.adobe.com/security/products/campaign/apsb21-52.html	O-MIC-WIND-081221/5953
Access of Memory	18-Nov-21	9.3	Adobe After Effects version 18.4 (and earlier) is affected	https://helpx.adobe.com	O-MIC-WIND-081221/5954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Location After End of Buffer			by a memory corruption vulnerability due to insecure handling of a malicious .m4a file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40751**	/security/products/after_effects/apsb21-79.html	
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious .m4a file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40752**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	O-MIC-WIND-081221/5955
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SVG file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	O-MIC-WIND-081221/5956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40753		
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40754**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	O-MIC-WIND-081221/5957
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SGI file in the DoReadContinue function, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. **CVE ID : CVE-2021-40755**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	O-MIC-WIND-081221/5958
NULL Pointer Dereference	18-Nov-21	4.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	O-MIC-WIND-081221/5959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-40756**		
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious MXF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40757**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	O-MIC-WIND-081221/5960
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40758**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	O-MIC-WIND-081221/5961
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious .m4a file, potentially resulting in arbitrary code execution in	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	O-MIC-WIND-081221/5962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40759**		
Access of Memory Location After End of Buffer	18-Nov-21	9.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious .m4a file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40760**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	O-MIC-WIND-081221/5963
NULL Pointer Dereference	18-Nov-21	4.3	Adobe After Effects version 18.4.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2021-40761**	https://helpx.adobe.com/security/products/after_effects/apsb21-79.html	O-MIC-WIND-081221/5964
Access of Memory Location	22-Nov-21	6.8	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption	https://helpx.adobe.com/security/pr	O-MIC-WIND-081221/5965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
After End of Buffer			vulnerability due to insecure handling of a malicious M4A file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40770**	oducts/prelude/apsb21-96.html	
Access of Memory Location After End of Buffer	22-Nov-21	6.8	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40771**	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	O-MIC-WIND-081221/5966
Access of Memory Location After End of Buffer	22-Nov-21	6.8	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious M4A file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40772**	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	O-MIC-WIND-081221/5967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	22-Nov-21	4.3	Adobe Prelude version 10.1 (and earlier) is affected by a null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2021-40773**	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	O-MIC-WIND-081221/5968
NULL Pointer Dereference	22-Nov-21	4.3	Adobe Prelude version 10.1 (and earlier) is affected by a null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2021-40774**	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	O-MIC-WIND-081221/5969
Access of Memory Location After End of Buffer	22-Nov-21	6.8	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SVG file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	O-MIC-WIND-081221/5970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-40775**		
Improper Resource Shutdown or Release	26-Nov-21	4.3	A vulnerability affecting F-Secure antivirus engine was discovered whereby unpacking UPX file can lead to denial-of-service. The vulnerability can be exploited remotely by an attacker. A successful attack will result in denial-of-service of the antivirus engine. **CVE ID : CVE-2021-40833**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40833	O-MIC-WIND-081221/5971
Out-of-bounds Write	18-Nov-21	9.3	Adobe Animate version 21.0.9 (and earlier) are affected by an out-of-bounds write 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 GIF file. **CVE ID : CVE-2021-42272**	https://helpx.adobe.com/security/products/animate/apsb21-105.html	O-MIC-WIND-081221/5972
Out-of-bounds Write	18-Nov-21	9.3	Adobe Animate version 21.0.9 (and earlier) are affected by an out-of-bounds write vulnerability that could result	https://helpx.adobe.com/security/products/anim	O-MIC-WIND-081221/5973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 BMP file. **CVE ID : CVE-2021-42524**	ate/apsb21-105.html	
Out-of-bounds Read	18-Nov-21	4.3	Acrobat Animate versions 21.0.9 (and earlier)is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-42525**	https://helpx.adobe.com/security/products/animate/apsb21-105.html	O-MIC-WIND-081221/5974
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Nov-21	9.3	Adobe Media Encoder version 15.4 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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 M4A file. **CVE ID : CVE-2021-42721**	https://helpx.adobe.com/security/products/media-encoder/apsb21-70.html	O-MIC-WIND-081221/5975
Access of Memory Location After End of Buffer	16-Nov-21	9.3	Adobe Premiere Pro version 15.4 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker	https://helpx.adobe.com/security/products/premiere_pro/a	O-MIC-WIND-081221/5976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to achieve 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 M4A file. **CVE ID : CVE-2021-42723**	psb21-67.html	
Access of Memory Location After End of Buffer	16-Nov-21	9.3	Adobe Media Encoder version 15.4 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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 M4A file. **CVE ID : CVE-2021-42726**	https://helpx.adobe.com/security/products/media-encoder/apsb21-70.html	O-MIC-WIND-081221/5977
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Nov-21	6.8	Acrobat RoboHelp Server versions 2020.0.1 (and earlier) are affected by a Path traversal vulnerability. The authenticated attacker can upload arbitrary files outside of the intended directory to cause remote code execution with privileges of user running Tomcat. Exploitation of this issue requires user interaction in that a victim must navigate to a planted file on the server. **CVE ID : CVE-2021-42727**	https://helpx.adobe.com/security/products/robohelp-server/apsb21-87.html	O-MIC-WIND-081221/5978
Buffer Copy	16-Nov-21	9.3	Adobe InDesign versions 16.4	https://help	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			(and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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-2021-42731**	x.adobe.com /security/products/indesign/apsb21-107.html	081221/5979
Improper Input Validation	22-Nov-21	6.8	Adobe Prelude version 10.1 (and earlier) is affected by an improper input validation vulnerability in the XDCAMSAM directory. An unauthenticated attacker could leverage this vulnerability to execute arbitrary code 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-2021-42733**	https://helpx.adobe.com /security/products/prelude/apsb21-96.html	O-MIC-WIND-081221/5980
Access of Memory Location After End of Buffer	22-Nov-21	6.8	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted	https://helpx.adobe.com /security/products/prelude/apsb21-96.html	O-MIC-WIND-081221/5981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file to exploit this vulnerability. **CVE ID : CVE-2021-42737**		
Access of Memory Location After End of Buffer	22-Nov-21	9.3	Adobe Prelude version 10.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious MXF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-42738**	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	O-MIC-WIND-081221/5982
Incorrect Authorization	17-Nov-21	4.6	Zoho Remote Access Plus Server Windows Desktop Binary fixed from 10.1.2121.1 is affected by incorrect access control. The installation directory is vulnerable to weak file permissions by allowing full control for Windows Everyone user group (non-admin or any guest users), thereby allowing privilege escalation, unauthorized password reset, stealing of sensitive data, access to credentials in plaintext, access to registry values, tampering with configuration files, etc. **CVE ID : CVE-2021-42954**	N/A	O-MIC-WIND-081221/5983
Incorrect Authorization	17-Nov-21	7.2	Zoho Remote Access Plus Server Windows Desktop binary fixed in version	N/A	O-MIC-WIND-081221/5984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.2132 is affected by an unauthorized password reset vulnerability. Because of the designed password reset mechanism, any non-admin Windows user can reset the password of the Remote Access Plus Server Admin account. **CVE ID : CVE-2021-42955**		
Improper Privilege Management	17-Nov-21	6.5	Zoho Remote Access Plus Server Windows Desktop Binary fixed in 10.1.2132.6 is affected by a sensitive information disclosure vulnerability. Due to improper privilege management, the process launches as the logged in user, so memory dump can be done by non-admin also. Remotely, an attacker can dump all sensitive information including DB Connection string, entire IT infrastructure details, commands executed by IT admin including credentials, secrets, private keys and more. **CVE ID : CVE-2021-42956**	N/A	O-MIC-WIND-081221/5985
Access of Memory Location After End of Buffer	16-Nov-21	9.3	Adobe Prelude version 10.1 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	O-MIC-WIND-081221/5986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requires user interaction in that a victim must open a malicious M4A file. **CVE ID : CVE-2021-43011**		
Access of Memory Location After End of Buffer	16-Nov-21	9.3	Adobe Prelude version 10.1 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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 M4A file. **CVE ID : CVE-2021-43012**	https://helpx.adobe.com/security/products/prelude/apsb21-96.html	O-MIC-WIND-081221/5987
Access of Memory Location After End of Buffer	16-Nov-21	9.3	Adobe Media Encoder version 15.4.1 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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-2021-43013**	https://helpx.adobe.com/security/products/media-encoder/apsb21-99.html	O-MIC-WIND-081221/5988
Access of Memory Location After End of Buffer	22-Nov-21	9.3	Adobe InCopy version 16.4 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious GIF file, potentially resulting in arbitrary code execution in	https://helpx.adobe.com/security/products/incopy/apsb21-110.html	O-MIC-WIND-081221/5989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability. **CVE ID : CVE-2021-43015**		
NULL Pointer Dereference	22-Nov-21	4.3	Adobe InCopy version 16.4 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2021-43016**	https://helpx.adobe.com/security/products/incopy/apsb21-110.html	O-MIC-WIND-081221/5990
Uncontrolled Search Path Element	29-Nov-21	4.4	DLL hijacking could lead to local privilege escalation. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035 **CVE ID : CVE-2021-44198**	https://security-advisory.acronis.com/advisories/SEC-2128	O-MIC-WIND-081221/5991
Uncontrolled Search Path Element	29-Nov-21	1.9	DLL hijacking could lead to denial of service. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27305, Acronis Cyber Protect Home Office (Windows) before build 39612	https://security-advisory.acronis.com/advisories/SEC-2508	O-MIC-WIND-081221/5992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-44199		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	Self cross-site scripting (XSS) was possible on devices page. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035 **CVE ID : CVE-2021-44200**	https://security-advisory.acronis.com/advisories/SEC-2803	O-MIC-WIND-081221/5993
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	4.3	Cross-site scripting (XSS) was possible in notification pop-ups. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035 **CVE ID : CVE-2021-44201**	https://security-advisory.acronis.com/advisories/SEC-3167	O-MIC-WIND-081221/5994
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	Stored cross-site scripting (XSS) was possible in activity details. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035 **CVE ID : CVE-2021-44202**	https://security-advisory.acronis.com/advisories/SEC-3283	O-MIC-WIND-081221/5995
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Nov-21	3.5	Stored cross-site scripting (XSS) was possible in protection plan details. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035 **CVE ID : CVE-2021-44203**	https://security-advisory.acronis.com/advisories/SEC-3294	O-MIC-WIND-081221/5996
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in an internal microcontroller which may allow a user with elevated privileges to generate valid	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-MIC-WIND-081221/5997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			microcode. This could lead to information disclosure, data corruption, or denial of service of the device. **CVE ID : CVE-2021-23201**		
N/A	20-Nov-21	7.2	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to instantiate a specifically timed DMA write to corrupt code execution, which may impact confidentiality, integrity, or availability. **CVE ID : CVE-2021-23217**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-MIC-WIND-081221/5998
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to access protected information, which may lead to information disclosure. **CVE ID : CVE-2021-23219**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-MIC-WIND-081221/5999
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to utilize debug mechanisms with insufficient access control, which may lead to information disclosure. **CVE ID : CVE-2021-1088**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-MIC-WIND-081221/6000
N/A	20-Nov-21	2.1	NVIDIA GPU and Tegra hardware contain a	https://nvidia.custhelp.c	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the internal microcontroller which may allow a user with elevated privileges to access debug registers during runtime, which may lead to information disclosure. **CVE ID : CVE-2021-1105**	om/app/answers/detail/a_id/5263	081221/6001
N/A	20-Nov-21	4.9	NVIDIA GPU and Tegra hardware contain a vulnerability in the internal microcontroller which may allow a user with elevated privileges to corrupt program data. **CVE ID : CVE-2021-1125**	https://nvidia.custhelp.com/app/answers/detail/a_id/5263	O-MIC-WIND-081221/6002
windows_10					
Improper Initialization	17-Nov-21	2.1	Improper initialization in the installer for some Intel(R) Graphics DCH Drivers for Windows 10 before version 27.20.100.9316 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2021-0120**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00566.html	O-MIC-WIND-081221/6003
Improper Privilege Management	17-Nov-21	4.6	Improper access control in the installer for some Intel(R) Iris(R) Xe MAX Dedicated Graphics Drivers for Windows 10 before version 27.20.100.9466 may allow authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0121**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00566.html	O-MIC-WIND-081221/6004
Untrusted Search Path	17-Nov-21	4.4	Uncontrolled search path in the Intel(R) RealSense(TM)	https://www.intel.com/	O-MIC-WIND-081221/6005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			D400 Series UWP driver for Windows 10 before version 6.1.160.22 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-33063**	content/www/us/en/security-center/advisory/intel-sa-00557.html	
Mitsubishielectric					
got2000_gt2103-pmbds2_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6006
got2000_gt2103-pmbds_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2103-pmbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6008
got2000_gt2103-pmbls_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all	https://www.mitsubishielectric.co.jp	O-MIT-GOT2-081221/6009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	/psirt/vulnerability/pdf/2021-018.pdf	
got2000_gt2104-rtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6010

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
got2000_gt2107-wtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6011
got2000_gt2308-vtba_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2308-vtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6013
got2000_gt2310-vtba_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2310-vtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6015
got2000_gt2505-vtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2505hs-vtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6017
got2000_gt2506hs-vtbd_firmware					
Improper Input	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000	https://www.mitsubishi	O-MIT-GOT2-081221/6018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	electric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	
got2000_gt2507-wtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction.	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20601		
got2000_gt2507-wtsd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6020
got2000_gt2507t-wtsd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2508-vtba_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6022
got2000_gt2508-vtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2508-vtwa_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6024
got2000_gt2508-vtwd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions,	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/	O-MIT-GOT2-081221/6025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	2021-018.pdf	
got2000_gt2510-vtba_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6026
got2000_gt2510-vtbd_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6027
got2000_gt2510-vtwa_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2510-vtwd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6029
got2000_gt2510-wxtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2510-wxtsd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6031
got2000_gt2512-stba_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2512-stbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6033
got2000_gt2512-wxtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all	https://www.mitsubishielectric.co.jp	O-MIT-GOT2-081221/6034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	/psirt/vulnerability/pdf/2021-018.pdf	
got2000_gt2512-wxtsd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6035

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
got2000_gt2705-vtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6036
got2000_gt2708-stba_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2708-stbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6038
got2000_gt2708-vtba_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2708-vtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6040
got2000_gt2710-stba_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2710-stbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6042
got2000_gt2710-vtba_firmware					
Improper Input	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000	https://www.mitsubishi	O-MIT-GOT2-081221/6043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	electric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	
got2000_gt2710-vtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction.	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20601		
got2000_gt2710-vtwa_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6045
got2000_gt2710-vtwd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2712-stba_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6047
got2000_gt2712-stbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got2000_gt2712-stwa_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6049
got2000_gt2712-stwd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions,	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/	O-MIT-GOT2-081221/6050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	2021-018.pdf	
got2000_gt2715-xtba_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6051
got2000_gt2715-xtbd_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT2-081221/6052
got_simple_gs2107-wtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT_-081221/6053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may be affected, such as malfunction. **CVE ID : CVE-2021-20601**		
got_simple_gs2110-wtbd_firmware					
Improper Input Validation	23-Nov-21	7.8	Improper input validation vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT23 model all versions, GOT2000 series GT21 model all versions, GOT SIMPLE series GS21 model all versions, and GT SoftGOT2000 all versions allows an remote unauthenticated attacker to write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction. **CVE ID : CVE-2021-20601**	https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2021-018.pdf	O-MIT-GOT_-081221/6054
ntt-west					
biz_box_nvr510_firmware					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page.	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://ww	O-NTT-BIZ_-081221/6055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20843	w.ntt-west.co.jp/smb/kiki_info/info/211109.html	
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	O-NTT-BIZ_-081221/6056
biz_box_nvr700w_firmware					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	O-NTT-BIZ_-081221/6057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	O-NTT-BIZ_-081221/6058
biz_box_rtx1210_firmware					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	O-NTT-BIZ_-081221/6059
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier,	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU9116	O-NTT-BIZ_-081221/6060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	1784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	
biz_box_rtx830_firmware					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	O-NTT-BIZ_-081221/6061
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/1	O-NTT-BIZ_-081221/6062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	1_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	
Oracle					
solaris					
Improper Restriction of Excessive Authentication Attempts	23-Nov-21	5	IBM Sterling Connect:Direct Web Services 1.0 and 6.0 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 209507. **CVE ID : CVE-2021-38890**	https://www.ibm.com/support/pages/node/6518586, https://exchange.xforce.ibmcloud.com/vulnerabilities/209507	O-ORA-SOLA-081221/6063
Inadequate Encryption Strength	23-Nov-21	5	IBM Sterling Connect:Direct Web Services 1.0 and 6.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 209508. **CVE ID : CVE-2021-38891**	https://www.ibm.com/support/pages/node/6518582, https://exchange.xforce.ibmcloud.com/vulnerabilities/209508	O-ORA-SOLA-081221/6064
Cleartext Storage of Sensitive Information	16-Nov-21	2.1	IBM MQ 7.5, 8.0, 9.0 LTS, 9.1 CD, and 9.1 LTS stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 211403. **CVE ID : CVE-2021-38949**	https://www.ibm.com/support/pages/node/6516424	O-ORA-SOLA-081221/6065
Philips					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mri_1.5t_firmware					
Exposure of Resource to Wrong Sphere	19-Nov-21	2.1	Philips MRI 1.5T and MRI 3T Version 5.x.x exposes sensitive information to an actor not explicitly authorized to have access. **CVE ID : CVE-2021-42744**	https://www.usa.philips.com/healthcare/about/customer-support/product-security	O-PHI-MRI_-081221/6066
Incorrect Ownership Assignment	19-Nov-21	2.1	Philips MRI 1.5T and MRI 3T Version 5.x.x assigns an owner who is outside the intended control sphere to a resource. **CVE ID : CVE-2021-26248**	https://www.usa.philips.com/healthcare/about/customer-support/product-security	O-PHI-MRI_-081221/6067
Improper Access Control	19-Nov-21	5	Philips MRI 1.5T and MRI 3T Version 5.x.x does not restrict or incorrectly restricts access to a resource from an unauthorized actor. **CVE ID : CVE-2021-26262**	https://www.usa.philips.com/healthcare/about/customer-support/product-security	O-PHI-MRI_-081221/6068
mri_3t_firmware					
Exposure of Resource to Wrong Sphere	19-Nov-21	2.1	Philips MRI 1.5T and MRI 3T Version 5.x.x exposes sensitive information to an actor not explicitly authorized to have access. **CVE ID : CVE-2021-42744**	https://www.usa.philips.com/healthcare/about/customer-support/product-security	O-PHI-MRI_-081221/6069
Incorrect Ownership Assignment	19-Nov-21	2.1	Philips MRI 1.5T and MRI 3T Version 5.x.x assigns an owner who is outside the intended control sphere to a resource.	https://www.usa.philips.com/healthcare/about/customer-	O-PHI-MRI_-081221/6070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26248	support/product-security	
Improper Access Control	19-Nov-21	5	Philips MRI 1.5T and MRI 3T Version 5.x.x does not restrict or incorrectly restricts access to a resource from an unauthorized actor. **CVE ID : CVE-2021-26262**	https://www.usa.philips.com/healthcare/about/customer-support/product-security	O-PHI-MRI_-081221/6071
Redhat					
enterprise_linux					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**	https://c-ares.haxx.se/adv_20210810.html	O-RED-ENTE-081221/6072
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Nov-21	5.1	When PgBouncer is configured to use "cert" authentication, a man-in-the-middle attacker can inject arbitrary SQL queries when a connection is first established, despite the use of TLS certificate verification and encryption. This flaw affects PgBouncer versions prior to 1.16.1. **CVE ID : CVE-2021-3935**	http://www.pgbouncer.org/changelog.html#pgbouncer-116x	O-RED-ENTE-081221/6073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
enterprise_linux_computer_node					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**	https://c-ares.haxx.se/adv_20210810.html	O-RED-ENTE-081221/6074
enterprise_linux_eus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**	https://c-ares.haxx.se/adv_20210810.html	O-RED-ENTE-081221/6075
enterprise_linux_for_ibm_z_systems					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to	https://c-ares.haxx.se/adv_20210810.html	O-RED-ENTE-081221/6076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**		
enterprise_linux_for_ibm_z_systems_eus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**	https://c-ares.haxx.se/adv_20210810.html	O-RED-ENTE-081221/6077
enterprise_linux_for_power_little_endian					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**	https://c-ares.haxx.se/adv_20210810.html	O-RED-ENTE-081221/6078
enterprise_linux_for_power_little_endian_eus					
Improper Neutralization of Input During Web Page Generation	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong	https://c-ares.haxx.se/adv_20210810.html	O-RED-ENTE-081221/6079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**		
enterprise_linux_server_aus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**	https://c-ares.haxx.se/adv_20210810.html	O-RED-ENTE-081221/6080
enterprise_linux_server_tus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**	https://c-ares.haxx.se/adv_20210810.html	O-RED-ENTE-081221/6081
enterprise_linux_server_update_services_for_sap_solutions					
Improper Neutralizatio	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input	https://c-ares.haxx.se	O-RED-ENTE-081221/6082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**	/adv_20210810.html	
enterprise_linux_tus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**	https://c-ares.haxx.se/adv_20210810.html	O-RED-ENTE-081221/6083
enterprise_linux_workstation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-21	7.5	A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3672**	https://c-ares.haxx.se/adv_20210810.html	O-RED-ENTE-081221/6084

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Samsung					
ddr4_sdram_firmware					
N/A	16-Nov-21	7.9	Modern DRAM devices (PC-DDR4, LPDDR4X) are affected by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer access patterns, consisting of aggressors with different frequencies, phases, and amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example, this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three major DRAM vendors	https://comsec.ethz.ch/wp-content/files/blacksmith_sp22.pdf	O-SAM-DDR4-081221/6085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Samsung, SK Hynix, Micron) are affected by this vulnerability. For more details, please refer to our publication. **CVE ID : CVE-2021-42114**		
lddr4_firmware					
N/A	16-Nov-21	7.9	Modern DRAM devices (PC-DDR4, LPDDR4X) are affected by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer access patterns, consisting of aggressors with different frequencies, phases, and amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example, this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-	https://comsec.ethz.ch/wp-content/files/blacksmith_sp22.pdf	O-SAM-LDDR-081221/6086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three major DRAM vendors (Samsung, SK Hynix, Micron) are affected by this vulnerability. For more details, please refer to our publication. **CVE ID : CVE-2021-42114**		
secomea					
gatemanager_8250_firmware					
N/A	22-Nov-21	5	This issue affects: Secomea GateManager All versions prior to 9.6. Improper Check of host header in web server of Secomea GateManager allows attacker to cause browser cache poisoning. **CVE ID : CVE-2021-32004**	https://www.secomea.com/support/cybersecurity-advisory/#4578	O-SEC-GATE-081221/6087
skhynix					
ddr4_sdram_firmware					
N/A	16-Nov-21	7.9	Modern DRAM devices (PC-DDR4, LPDDR4X) are affected by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer access patterns, consisting of aggressors with different frequencies, phases, and amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were	https://comsec.ethz.ch/wp-content/files/blacksmith_sp22.pdf	O-SKH-DDR4-081221/6088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example, this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three major DRAM vendors (Samsung, SK Hynix, Micron) are affected by this vulnerability. For more details, please refer to our publication. **CVE ID : CVE-2021-42114**		
lddr4_firmware					
N/A	16-Nov-21	7.9	Modern DRAM devices (PC-DDR4, LPDDR4X) are affected by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks. Novel non-uniform Rowhammer access patterns, consisting of aggressors with different frequencies, phases, and	https://comsec.ethz.ch/wp-content/files/blacksmith_sp22.pdf	O-SKH-LDDR-081221/6089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			amplitudes allow triggering bit flips on affected memory modules using our Blacksmith fuzzer. The patterns generated by Blacksmith were able to trigger bitflips on all 40 PC-DDR4 DRAM devices in our test pool, which cover the three major DRAM manufacturers: Samsung, SK Hynix, and Micron. This means that, even when chips advertised as Rowhammer-free are used, attackers may still be able to exploit Rowhammer. For example, this enables privilege-escalation attacks against the kernel or binaries such as the sudo binary, and also triggering bit flips in RSA-2048 keys (e.g., SSH keys) to gain cross-tenant virtual-machine access. We can confirm that DRAM devices acquired in July 2020 with DRAM chips from all three major DRAM vendors (Samsung, SK Hynix, Micron) are affected by this vulnerability. For more details, please refer to our publication. **CVE ID : CVE-2021-42114**		
Windriver					
vxworks					
Double Free	24-Nov-21	5	An issue was discovered in VxWorks 6.9 through 7. In the IKE component, a specifically crafted packet may lead to	https://support2.windriver.com/index.php?page=	O-WIN-VXWO-081221/6090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reading beyond the end of a buffer, or a double free. **CVE ID : CVE-2021-43268**	cve&on=view&id=CVE-2021-43268	
XEN					
xen					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-21	6.9	PoD operations on misaligned GFNs T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] x86 HVM and PVH guests may be started in populate-on-demand (PoD) mode, to provide a way for them to later easily have more memory assigned. Guests are permitted to control certain P2M aspects of individual pages via hypercalls. These hypercalls may act on ranges of pages specified via page orders (resulting in a power-of-2 number of pages). The implementation of some of these hypercalls for PoD does not enforce the base page frame number to be suitably aligned for the specified order, yet some code involved in PoD handling actually makes such an assumption. These operations are XENMEM_decrease_reservation (CVE-2021-28704) and XENMEM_populate_physmap (CVE-2021-28707), the latter usable only by domains controlling the guest, i.e. a de-privileged qemu or a stub	https://xenbits.xenproject.org/xsa/advisory-388.txt	O-XEN-XEN-081221/6091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			domain. (Patch 1, combining the fix to both these two issues.) In addition handling of XENMEM_decrease_reservation can also trigger a host crash when the specified page order is neither 4k nor 2M nor 1G (CVE-2021-28708, patch 2). **CVE ID : CVE-2021-28704**		
Improper Handling of Exceptional Conditions	24-Nov-21	6.9	issues with partially successful P2M updates on x86 T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] x86 HVM and PVH guests may be started in populate-on-demand (PoD) mode, to provide a way for them to later easily have more memory assigned. Guests are permitted to control certain P2M aspects of individual pages via hypercalls. These hypercalls may act on ranges of pages specified via page orders (resulting in a power-of-2 number of pages). In some cases the hypervisor carries out the requests by splitting them into smaller chunks. Error handling in certain PoD cases has been insufficient in that in particular partial success of some operations was not properly accounted for. There are two code paths affected -	https://xenbits.xenproject.org/xsa/advisory-389.txt	O-XEN-XEN-081221/6092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			page removal (CVE-2021-28705) and insertion of new pages (CVE-2021-28709). (We provide one patch which combines the fix to both issues.) **CVE ID : CVE-2021-28705**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-21	6.9	PoD operations on misaligned GFNs T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] x86 HVM and PVH guests may be started in populate-on-demand (PoD) mode, to provide a way for them to later easily have more memory assigned. Guests are permitted to control certain P2M aspects of individual pages via hypercalls. These hypercalls may act on ranges of pages specified via page orders (resulting in a power-of-2 number of pages). The implementation of some of these hypercalls for PoD does not enforce the base page frame number to be suitably aligned for the specified order, yet some code involved in PoD handling actually makes such an assumption. These operations are XENMEM_decrease_reservation (CVE-2021-28704) and XENMEM_populate_physmap (CVE-2021-28707), the latter usable only by domains	https://xenbits.xenproject.org/xsa/advisory-388.txt	O-XEN-XEN-081221/6093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controlling the guest, i.e. a de-privileged qemu or a stub domain. (Patch 1, combining the fix to both these two issues.) In addition handling of XENMEM_decrease_reservation can also trigger a host crash when the specified page order is neither 4k nor 2M nor 1G (CVE-2021-28708, patch 2). **CVE ID : CVE-2021-28707**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-21	6.9	PoD operations on misaligned GFNs T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] x86 HVM and PVH guests may be started in populate-on-demand (PoD) mode, to provide a way for them to later easily have more memory assigned. Guests are permitted to control certain P2M aspects of individual pages via hypercalls. These hypercalls may act on ranges of pages specified via page orders (resulting in a power-of-2 number of pages). The implementation of some of these hypercalls for PoD does not enforce the base page frame number to be suitably aligned for the specified order, yet some code involved in PoD handling actually makes such an assumption. These operations are	https://xenbits.xenproject.org/xsa/advisory-388.txt	O-XEN-XEN-081221/6094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			XENMEM_decrease_reservation (CVE-2021-28704) and XENMEM_populate_physmap (CVE-2021-28707), the latter usable only by domains controlling the guest, i.e. a de-privileged qemu or a stub domain. (Patch 1, combining the fix to both these two issues.) In addition handling of XENMEM_decrease_reservation can also trigger a host crash when the specified page order is neither 4k nor 2M nor 1G (CVE-2021-28708, patch 2). **CVE ID : CVE-2021-28708**		
Improper Handling of Exceptional Conditions	24-Nov-21	6.9	issues with partially successful P2M updates on x86 T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] x86 HVM and PVH guests may be started in populate-on-demand (PoD) mode, to provide a way for them to later easily have more memory assigned. Guests are permitted to control certain P2M aspects of individual pages via hypercalls. These hypercalls may act on ranges of pages specified via page orders (resulting in a power-of-2 number of pages). In some cases the hypervisor carries out the requests by splitting them into smaller	https://xenbits.xenproject.org/xsa/advisory-389.txt	O-XEN-XEN-081221/6095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			chunks. Error handling in certain PoD cases has been insufficient in that in particular partial success of some operations was not properly accounted for. There are two code paths affected - page removal (CVE-2021-28705) and insertion of new pages (CVE-2021-28709). (We provide one patch which combines the fix to both issues.) **CVE ID : CVE-2021-28709**		
Improper Privilege Management	21-Nov-21	6.9	certain VT-d IOMMUs may not work in shared page table mode For efficiency reasons, address translation control structures (page tables) may (and, on suitable hardware, by default will) be shared between CPUs, for second-level translation (EPT), and IOMMUs. These page tables are presently set up to always be 4 levels deep. However, an IOMMU may require the use of just 3 page table levels. In such a configuration the lop level table needs to be stripped before inserting the root table's address into the hardware pagetable base register. When sharing page tables, Xen erroneously skipped this stripping. Consequently, the guest is able to write to leaf page table entries. **CVE ID : CVE-2021-28710**	https://xenbits.xenproject.org/xsa/advisory-390.txt	O-XEN-XEN-081221/6096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Yamaha					
nvr510_firmware					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	O-YAM-NVR5-081221/6097
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	O-YAM-NVR5-081221/6098
nvr700w_firmware					
Inclusion of Functionality	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI	http://www.rtpro.yamah	O-YAM-NVR7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
from Untrusted Control Sphere			of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	a.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	081221/6099
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	O-YAM-NVR7-081221/6100
rtx1210_firmware					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://busi	O-YAM-RTX1-081221/6101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page. **CVE ID : CVE-2021-20843**	ness.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	O-YAM-RTX1-081221/6102
rtx830_firmware					
Inclusion of Functionality from Untrusted Control Sphere	24-Nov-21	3.5	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page.	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://ww	O-YAM-RTX8-081221/6103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20843	w.ntt-west.co.jp/smb/kiki_info/info/211109.html	
Improper Encoding or Escaping of Output	24-Nov-21	3.5	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page. **CVE ID : CVE-2021-20844**	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html, https://business.ntt-east.co.jp/topics/2021/11_09.html, https://www.ntt-west.co.jp/smb/kiki_info/info/211109.html	O-YAM-RTX8-081221/6104