Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
10web					
form_maker					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	The Form Maker by 10Web â€“ Mobile-Friendly Drag & Drop Contact Form Builder WordPress plugin before 1.13.60 does not escape its Form Title before outputting it in an attribute when editing a form in the admin dashboard, leading to an authenticated Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24526**	N/A	A-10W-FORM-020921/1
photo_gallery					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The Photo Gallery by 10Web â€“ Mobile-Friendly Image Gallery WordPress plugin before 1.5.75 did not ensure that uploaded SVG files added to a gallery do not contain malicious content. As a result, users allowed to add images to gallery can upload an SVG file containing JavaScript code, which will be executed when accessing the image directly (ie in the /wp-content/uploads/photo-gallery/ folder), leading to a Cross-Site Scripting (XSS) issue **CVE ID : CVE-2021-24362**	N/A	A-10W-PHOT-020921/2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Aug-21	4	The Photo Gallery by 10Web â€“ Mobile-Friendly Image Gallery WordPress plugin before 1.5.75 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images/SVG anywhere in the filesystem via a path traversal vector **CVE ID : CVE-2021-24363**	N/A	A-10W-PHOT-020921/3
3.7designs					
project_status					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	3.5	The pspin_duplicate_post_save_as_new_post function of the Project Status WordPress plugin through 1.6 does not sanitise, validate or escape the post GET parameter passed to it before outputting it in an error message when the related post does not exist, leading to a reflected XSS issue **CVE ID : CVE-2021-24558**	N/A	A-3.7-PROJ-020921/4
aceide_project					
aceide					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Aug-21	4	The AceIDE WordPress plugin through 2.6.2 does not sanitise or validate the user input which is appended to system paths before using it in various actions, such as to read arbitrary files from the server. This allows high privilege users such as administrator to access any file on the web server outside of the blog	N/A	A-ACE-ACEI-020921/5

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			directory via a path traversal attack. **CVE ID : CVE-2021-24549**		
add_sidebar_project					
add_sidebar					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The Add Sidebar WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the add parameter in the ~/wp_sidebarMenu.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.0. **CVE ID : CVE-2021-34666**	N/A	A-ADD-ADD_-020921/6
Adobe					
acrobat_dc					
Use After Free	20-Aug-21	6	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by an Use-after-free vulnerability. An authenticated 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-2021-28640**	https://helpx.adobe.com/security/products/acrobat/apsb21-51.html	A-ADO-ACRO-020921/7
Use After Free	20-Aug-21	6.8	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by an Use-after-free vulnerability. An	https://helpx.adobe.com/security/products/acrobat/apsb21-51.html	A-ADO-ACRO-020921/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2021-28641**		
Out-of-bounds Write	20-Aug-21	6.8	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by an Out-of-bounds write 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-2021-28642**	https://helpx.adobe.com/security/products/acrobat/apsb21-51.html	A-ADO-ACRO-020921/9
Access of Resource Using Incompatible Type ('Type Confusion')	20-Aug-21	4.3	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by a Type Confusion vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive 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.	https://helpx.adobe.com/security/products/acrobat/apsb21-51.html	A-ADO-ACRO-020921/10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28643		
acrobat_reader_dc					
Use After Free	20-Aug-21	6	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by an Use-after-free vulnerability. An authenticated 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-2021-28640**	https://helpx.adobe.com/security/products/acrobat/apsb21-51.html	A-ADO-ACRO-020921/11
Use After Free	20-Aug-21	6.8	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by an Use-after-free 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-2021-28641**	https://helpx.adobe.com/security/products/acrobat/apsb21-51.html	A-ADO-ACRO-020921/12
Out-of-bounds Write	20-Aug-21	6.8	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by an Out-of-bounds write vulnerability. An unauthenticated attacker	https://helpx.adobe.com/security/products/acrobat/apsb21-51.html	A-ADO-ACRO-020921/13

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 file. **CVE ID : CVE-2021-28642**		
Access of Resource Using Incompatible Type ('Type Confusion')	20-Aug-21	4.3	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by a Type Confusion vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive 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-2021-28643**	https://helpx.adobe.com/security/products/acrobat/apsb21-51.html	A-ADO-ACRO-020921/14
after_effects					
Out-of-bounds Read	24-Aug-21	5.8	Adobe After Effects version 18.2 (and earlier) is affected by an Our-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information and cause a 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.	https://helpx.adobe.com/security/products/after_effects/apsb21-49.html	A-ADO-AFTE-020921/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28612		
Out-of-bounds Read	24-Aug-21	5.8	Adobe After Effects version 18.2 (and earlier) is affected by an Our-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information and cause a 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-2021-28614**	https://helpx.adobe.com/security/products/after_effects/apsb21-49.html	A-ADO-AFTE-020921/16
animate					
Out-of-bounds Read	24-Aug-21	4.3	Adobe Animate version 21.0.6 (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 sensitive 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-2021-28619**	https://helpx.adobe.com/security/products/animate/apsb21-50.html	A-ADO-ANIM-020921/17
Heap-based Buffer Overflow	24-Aug-21	6.8	Adobe Animate version 21.0.6 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/animate/apsb21-50.html	A-ADO-ANIM-020921/18

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-28620**		
Out-of-bounds Read	24-Aug-21	6.8	Adobe Animate version 21.0.6 (and earlier) is affected by an Out-of-bounds Read 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-2021-28621**	https://helpx.adobe.com/security/products/animate/apsb21-50.html	A-ADO-ANIM-020921/19
Out-of-bounds Write	24-Aug-21	6.8	Adobe Animate version 21.0.6 (and earlier) is affected by an Out-of-bounds Write 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-2021-28622**	https://helpx.adobe.com/security/products/animate/apsb21-50.html	A-ADO-ANIM-020921/20
Heap-based Buffer Overflow	24-Aug-21	6.8	Adobe Animate version 21.0.6 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/animate/apsb21-50.html	A-ADO-ANIM-020921/21

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-28629**		
Out-of-bounds Read	24-Aug-21	6.8	Adobe Animate version 21.0.6 (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 potential sensitive 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-2021-28630**	https://helpx.adobe.com/security/products/animate/apsb21-50.html	A-ADO-ANIM-020921/22
bridge					
Heap-based Buffer Overflow	20-Aug-21	9.3	Adobe Bridge version 11.0.2 (and earlier) are affected by a Heap-based Buffer overflow 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-2021-28624**	https://helpx.adobe.com/security/products/bridge/apsb21-53.html	A-ADO-BRID-020921/23
Out-of-bounds Write	20-Aug-21	9.3	Adobe Bridge version 11.0.2 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a specially crafted file. An unauthenticated attacker could	https://helpx.adobe.com/security/products/bridge/apsb21-53.html	A-ADO-BRID-020921/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2021-35989**		
Out-of-bounds Write	20-Aug-21	9.3	Adobe Bridge version 11.0.2 (and earlier) is affected by an Out-of-bounds Write 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-2021-35990**	https://helpx.adobe.com/security/products/bridge/apsb21-53.html	A-ADO-BRID-020921/25
Improper Input Validation	20-Aug-21	4.3	Adobe Bridge version 11.0.2 (and earlier) is affected by an uninitialized variable 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-2021-35991**	https://helpx.adobe.com/security/products/bridge/apsb21-53.html	A-ADO-BRID-020921/26
Out-of-bounds Read	20-Aug-21	4.3	Adobe Bridge version 11.0.2 (and earlier) is affected by an Out-of-bounds Read	https://helpx.adobe.com/security/prod	A-ADO-BRID-020921/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive 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-2021-35992**	ucts/bridge/apsb21-53.html	
character_animator					
Access of Memory Location After End of Buffer	20-Aug-21	9.3	Adobe Character Animator version 4.2 (and earlier) is affected by a memory corruption 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-2021-36000**	https://helpx.adobe.com/in/security/products/character_animator/apsb21-59.html	A-ADO-CHAR-020921/28
Out-of-bounds Read	20-Aug-21	4.3	Adobe Character Animator version 4.2 (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	https://helpx.adobe.com/in/security/products/character_animator/apsb21-59.html	A-ADO-CHAR-020921/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that a victim must open a malicious file. **CVE ID : CVE-2021-36001**		
dimension					
Uncontrolled Search Path Element	20-Aug-21	9.3	Adobe Dimension version 3.4 (and earlier) is affected by an Uncontrolled Search Path Element element. 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-2021-28595**	https://helpx.adobe.com/security/products/dimension/apsb21-40.html	A-ADO-DIME-020921/30
framemaker					
Out-of-bounds Write	23-Aug-21	9.3	Adobe Framemaker version 2020.0.1 (and earlier) and 2019.0.8 (and earlier) are affected by an Out-of-bounds Write 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-2021-28596**	https://helpx.adobe.com/security/products/framemaker/apsb21-45.html	A-ADO-FRAM-020921/31
illustrator					
Out-of-bounds Write	20-Aug-21	6.8	Adobe Illustrator version 25.2.3 (and earlier) is affected by an Out-of-bounds Write	https://helpx.adobe.com/security/prod	A-ADO-ILLU-020921/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2021-28591**	ucts/illustrator/apsb21-42.html	
Out-of-bounds Write	20-Aug-21	6.8	Adobe Illustrator version 25.2.3 (and earlier) is affected by an Out-of-bounds Write 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-2021-28592**	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	A-ADO-ILLU-020921/33
Use After Free	20-Aug-21	4.3	Adobe Illustrator version 25.2.3 (and earlier) is affected by a Use After Free vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose potential sensitive 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-2021-28593**	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	A-ADO-ILLU-020921/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	20-Aug-21	4.3	Adobe Illustrator version 25.2.3 (and earlier) is affected by an Use-after-free vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to read arbitrary file system 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-2021-36008**	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	A-ADO-ILLU-020921/35
Access of Memory Location After End of Buffer	20-Aug-21	9.3	Adobe Illustrator version 25.2.3 (and earlier) is affected by an memory corruption 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-2021-36009**	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	A-ADO-ILLU-020921/36
Out-of-bounds Read	20-Aug-21	4.3	Adobe Illustrator version 25.2.3 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of 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.	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	A-ADO-ILLU-020921/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36010		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Aug-21	9.3	Adobe Illustrator version 25.2.3 (and earlier) is affected by a potential Command injection vulnerability when chained with a development and debugging tool for JavaScript scripts. 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-2021-36011**	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	A-ADO-ILLU-020921/38
media_encoder					
Out-of-bounds Read	20-Aug-21	6.8	Adobe Media Encoder version 15.2 (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 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-2021-28589**	https://helpx.adobe.com/security/products/media-encoder/apsb21-43.html	A-ADO-MEDI-020921/39
Out-of-bounds Read	20-Aug-21	6.8	Adobe Media Encoder version 15.2 (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	https://helpx.adobe.com/security/products/media-encoder/apsb21-43.html	A-ADO-MEDI-020921/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2021-28590**		
Out-of-bounds Read	23-Aug-21	6.8	Adobe Media Encoder version 15.2 (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 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-2021-36013**	https://helpx.adobe.com/security/products/media-encoder/apsb21-43.html	A-ADO-MEDI-020921/41
Access of Uninitialized Pointer	20-Aug-21	4.3	Adobe Media Encoder version 15.2 (and earlier) is affected by an uninitialized pointer vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to read arbitrary file system 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-2021-36014**	https://helpx.adobe.com/security/products/media-encoder/apsb21-43.html	A-ADO-MEDI-020921/42
Access of Memory Location After End of	20-Aug-21	9.3	Adobe Media Encoder version 15.2 (and earlier) is affected by a memory corruption vulnerability when parsing a	https://helpx.adobe.com/security/products/media-	A-ADO-MEDI-020921/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			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-2021-36015**	encoder/apsb21-43.html	
Out-of-bounds Read	20-Aug-21	4.3	Adobe Media Encoder version 15.2 (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 read arbitrary file system 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-2021-36016**	https://helpx.adobe.com/security/products/media-encoder/apsb21-43.html	A-ADO-MEDI-020921/44
photoshop					
Stack-based Buffer Overflow	20-Aug-21	9.3	Adobe Photoshop versions 21.2.9 (and earlier) and 22.4.2 (and earlier) is affected by a stack overflow vulnerability due to insecure handling of a crafted PSD file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted PSD file in Photoshop. **CVE ID : CVE-2021-36005**	https://helpx.adobe.com/security/products/photoshop/apsb21-63.html	A-ADO-PHOT-020921/45
Improper	20-Aug-21	4.3	Adobe Photoshop versions	https://helpx	A-ADO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			21.2.9 (and earlier) and 22.4.2 (and earlier) are affected by an Improper input validation 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-2021-36006**	.adobe.com/security/products/photoshop/apsb21-63.html	PHOT-020921/46
prelude					
Access of Memory Location After End of Buffer	20-Aug-21	9.3	Adobe Prelude version 10.0 (and earlier) is affected by a memory corruption 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-2021-35999**	https://helpx.adobe.com/security/products/prelude/apsb21-58.html	A-ADO-PREL-020921/47
Use of Uninitialized Resource	20-Aug-21	6.8	Adobe Prelude version 10.0 (and earlier) are affected by an uninitialized variable 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	https://helpx.adobe.com/security/products/prelude/apsb21-58.html	A-ADO-PREL-020921/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-36007**		
premiere_pro					
Access of Memory Location After End of Buffer	20-Aug-21	9.3	Adobe Premiere Pro version 15.2 (and earlier) is affected by a memory corruption 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-2021-35997**	https://helpx.adobe.com/security/products/premiere_pro/apsb21-56.html	A-ADO-PREM-020921/49
ansi-html_project					
ansi-html					
N/A	18-Aug-21	5	This affects all versions of package ansi-html. If an attacker provides a malicious string, it will get stuck processing the input for an extremely long time. **CVE ID : CVE-2021-23424**	N/A	A-ANS-ANSI-020921/50
Apache					
airflow					
Missing Authorization	16-Aug-21	5	If remote logging is not used, the worker (in the case of CeleryExecutor) or the scheduler (in the case of LocalExecutor) runs a Flask logging server and is listening on a specific port and also	https://lists.apache.org/thread.html/r53d6bd7b0a66f92ddaf1313282f10fec802e712466	A-APA-AIRF-020921/51

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			binds on 0.0.0.0 by default. This logging server had no authentication and allows reading log files of DAG jobs. This issue affects Apache Airflow < 2.1.2. **CVE ID : CVE-2021-35936**	06dd30c16536df%40%3Cusers.airflow.apache.org%3E	
http_server					
N/A	16-Aug-21	5	A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48. **CVE ID : CVE-2021-33193**	https://github.com/apache/httpd/commit/ecebcc035ccd8d0e2984fe41420d9e944f456b3c.patch	A-APA-HTTP-020921/52
ofbiz					
Unrestricted Upload of File with Dangerous Type	18-Aug-21	7.5	Unrestricted Upload of File with Dangerous Type vulnerability in Apache OFBiz allows an attacker to execute remote commands. This issue affects Apache OFBiz version 17.12.07 and prior versions. Upgrade to at least 17.12.08 or apply patches at https://issues.apache.org/jira/browse/OFBIZ-12297. **CVE ID : CVE-2021-37608**	https://ofbiz.apache.org/security.html	A-APA-OFBI-020921/53
portable_runtime					
Out-of-bounds Read	23-Aug-21	3.6	An out-of-bounds array read in the apr_time_exp*() functions was fixed in the Apache Portable Runtime 1.6.3 release (CVE-2017-12613). The fix for this issue was not carried forward to the APR 1.7.x	http://mail-archives.apache.org/mod_mbox/www-announce/201710.mbox/%3CCACsi25	A-APA-PORT-020921/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			branch, and hence version 1.7.0 regressed compared to 1.6.3 and is vulnerable to the same issue. **CVE ID : CVE-2021-35940**	1B8UaLvM-rrH9fv57-zWi0zhyF3275_jPg1a9VEVVoxw@mail.gmail.com%3E, http://svn.apache.org/viewvc?view=revision&revision=1891198	
roller					
Uncontrolled Resource Consumption	18-Aug-21	4.3	User controlled `request.getHeader("Referer")` , `request.getRequestURL()` and `request.getQueryString()` are used to build and run a regex expression. The attacker doesn't have to use a browser and may send a specially crafted Referer header programmatically. Since the attacker controls the string and the regex pattern he may cause a ReDoS by regex catastrophic backtracking on the server side. This problem has been fixed in Roller 6.0.2. **CVE ID : CVE-2021-33580**	https://lists.apache.org/thread.html/r9d967d80af941717573e531db2c7353a90bfd0886e9b5d5d79f75506%40%3Cuser.roller.apache.org%3E	A-APA-ROLL-020921/55
arvtard					
jquery_tagline_rotator					
Improper Neutralization of Input During Web Page Generation ('Cross-site	16-Aug-21	4.3	The jQuery Tagline Rotator WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of $_SERVER['PHP_SELF'] in the ~/jquery-tagline-rotator.php file which allows attackers to	N/A	A-ARV-JQUE-020921/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			inject arbitrary web scripts, in versions up to and including 0.1.5. **CVE ID : CVE-2021-34663**		
Atlassian					
data_center					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Aug-21	5	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to read particular files via a path traversal vulnerability in the /WEB-INF/web.xml endpoint. The affected versions are before version 8.5.14, from version 8.6.0 before 8.13.6, and from version 8.14.0 before 8.16.1. **CVE ID : CVE-2021-26086**	https://jira.atlassian.com/browse/JRASERVER-72695	A-ATL-DATA-020921/57
URL Redirection to Untrusted Site ('Open Redirect')	25-Aug-21	4.9	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to redirect users to a malicious URL via a reverse tabnapping vulnerability in the Project Shortcuts feature. The affected versions are before version 8.5.15, from version 8.6.0 before 8.13.7, from version 8.14.0 before 8.17.1, and from version 8.18.0 before 8.18.1. **CVE ID : CVE-2021-39112**	https://jira.atlassian.com/browse/JRASERVER-72433	A-ATL-DATA-020921/58
jira					
Improper Limitation of a Pathname to a Restricted Directory	16-Aug-21	5	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to read particular files via a path traversal vulnerability in the /WEB-INF/web.xml endpoint.	https://jira.atlassian.com/browse/JRASERVER-72695	A-ATL-JIRA-020921/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			The affected versions are before version 8.5.14, from version 8.6.0 before 8.13.6, and from version 8.14.0 before 8.16.1. **CVE ID : CVE-2021-26086**		
URL Redirection to Untrusted Site ('Open Redirect')	25-Aug-21	4.9	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to redirect users to a malicious URL via a reverse tabnapping vulnerability in the Project Shortcuts feature. The affected versions are before version 8.5.15, from version 8.6.0 before 8.13.7, from version 8.14.0 before 8.17.1, and from version 8.18.0 before 8.18.1. **CVE ID : CVE-2021-39112**	https://jira.atlassian.com/browse/JRASERVER-72433	A-ATL-JIRA-020921/60
ATT					
xmill					
Out-of-bounds Write	17-Aug-21	7.5	A memory corruption vulnerability exists in the XML-parsing ParseAttribs functionality of AT&T Labs' Xmill 0.7. A specially crafted XML file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21810**	N/A	A-ATT-XMIL-020921/61
Out-of-bounds Write	18-Aug-21	7.5	A heap-based buffer overflow vulnerability exists in the XML Decompression PlainTextUncompressor::UncompressItem functionality of AT&T Labs' Xmill 0.7. A specially crafted XMI file can	N/A	A-ATT-XMIL-020921/62

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to remote code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21825**		
Out-of-bounds Write	20-Aug-21	7.5	A heap-based buffer overflow vulnerability exists in the XML Decompression DecodeTreeBlock functionality of AT&T Labs Xmill 0.7. Within `DecodeTreeBlock` which is called during the decompression of an XMI file, a UINT32 is loaded from the file and used as trusted input as the length of a buffer. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21826**	N/A	A-ATT-XMIL-020921/63
Out-of-bounds Write	20-Aug-21	7.5	A heap-based buffer overflow vulnerability exists in the XML Decompression DecodeTreeBlock functionality of AT&T Labs Xmill 0.7. Within `DecodeTreeBlock` which is called during the decompression of an XMI file, a UINT32 is loaded from the file and used as trusted input as the length of a buffer. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21827**	N/A	A-ATT-XMIL-020921/64
Out-of-bounds Write	20-Aug-21	7.5	A heap-based buffer overflow vulnerability exists in the XML Decompression DecodeTreeBlock functionality	N/A	A-ATT-XMIL-020921/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of AT&T Labs Xmill 0.7. In the default case of DecodeTreeBlock a label is created via CurPath::AddLabel in order to track the label for later reference. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21828**		
awplife					
grid_gallery					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	3.5	The Grid Gallery â€“ Photo Image Grid Gallery WordPress plugin before 1.2.5 does not properly sanitize the title field for image galleries when adding them via the admin dashboard, resulting in an authenticated Stored Cross-Site Scripting vulnerability. **CVE ID : CVE-2021-24529**	N/A	A-AWP-GRID-020921/66
Basercms					
basercms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Aug-21	3.5	baserCMS is an open source content management system with a focus on Japanese language support. In affected versions there is a cross-site scripting vulnerability in the file upload function of the management system of baserCMS. Users are advised to update as soon as possible. No workaround are available to mitigate this issue. **CVE ID : CVE-2021-39136**	https://github.com/baserproject/basercms/commit/568d4cab5ba1cdee7bbf0133c676d02a98f6d7bc, https://github.com/baserproject/basercms/security/advisories/GHSA-hgjr-632x-qpp3,	A-BAS-BASE-020921/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://basercms.net/security/JVN_14134801	
baserow					
baserow					
Server-Side Request Forgery (SSRF)	20-Aug-21	4	SSRF in URL file upload in Baserow <1.1.0 allows remote authenticated users to retrieve files from the internal server network exposed over HTTP by inserting an internal address. **CVE ID : CVE-2021-22255**	https://gitlab.com/bramw/baserow/-/issues/370, https://baserow.io/blog/march-2021-release-of-baserow, https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22255.json	A-BAS-BASE-020921/68
bblfshd_project					
bblfshd					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Aug-21	5.5	bblfshd is an open source self-hosted server for source code parsing. In bblfshd before commit 4265465b9b6fb5663c30ee43806126012066aad4 there is a "zipslip" vulnerability. The unsafe handling of symbolic links in an unpacking routine may enable attackers to read and/or write to arbitrary locations outside the designated target folder. This issue may lead to arbitrary file write (with same permissions	https://github.com/bblfsh/bblfshd/pull/341, https://securitylab.github.com/advisories/GHSL-2020-258-zipslip-bblfshd/, https://github.com/bblfsh/bblfshd/commit/42654	A-BBL-BBLF-020921/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as the program running the unpack operation) if the attacker can control the archive file. Additionally, if the attacker has read access to the unpacked files, he may be able to read arbitrary system files the parent process has permissions to read. For more details including a PoC see the referenced GHSL-2020-258. **CVE ID : CVE-2021-32825**	65b9b6fb5663c30ee43806126012066aad4	
bikeshed_project					
bikeshed					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Aug-21	6.8	This affects the package bikeshed before 3.0.0. This can occur when an untrusted source file containing Inline Tag Command metadata is processed. When an arbitrary OS command is executed, the command output would be included in the HTML output. **CVE ID : CVE-2021-23422**	https://snyk.io/vuln/SNYK-PYTHON-BIKESHED-1537646, https://github.com/tabatkins/bikeshed/commit/b2f668fca204260b1cad28d5078e93471cb6b2dd	A-BIK-BIKE-020921/70
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Aug-21	5	This affects the package bikeshed before 3.0.0. This can occur when an untrusted source file containing include, include-code or include-raw block is processed. The contents of arbitrary files could be disclosed in the HTML output. **CVE ID : CVE-2021-23423**	https://snyk.io/vuln/SNYK-PYTHON-BIKESHED-1537647, https://github.com/tabatkins/bikeshed/commit/b2f668fca204260b1cad28d5078e93471c	A-BIK-BIKE-020921/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				b6b2dd	
Blackberry					
qnx_software_development_platform					
Integer Overflow or Wraparound	17-Aug-21	6.8	An integer overflow vulnerability in the calloc() function of the C runtime library of affected versions of BlackBerry® QNX Software Development Platform (SDP) version(s) 6.5.0SP1 and earlier, QNX OS for Medical 1.1 and earlier, and QNX OS for Safety 1.0.1 and earlier that could allow an attacker to potentially perform a denial of service or execute arbitrary code. **CVE ID : CVE-2021-22156**	https://support.blackberry.com/kb/articleDetail?articleNumber=000082334	A-BLA-QNX_-020921/72
broken_link_manager_project					
broken_link_manager					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-21	6.5	The Broken Link Manager WordPress plugin through 0.6.5 does not sanitise, validate or escape the url GET parameter before using it in a SQL statement when retrieving an URL to edit, leading to an authenticated SQL injection issue **CVE ID : CVE-2021-24550**	N/A	A-BRO-BROK-020921/73
calendar_plugin_project					
calendar_plugin					
Improper Neutralization of Input During Web Page	16-Aug-21	4.3	The Calendar_plugin WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of `$_SERVER['PHP_SELF']` in the	N/A	A-CAL-CALE-020921/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			~/calendar.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0. **CVE ID : CVE-2021-34667**		
Canon					
oce_print_exec_workgroup					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	4.3	Canon Oce Print Exec Workgroup 1.3.2 allows XSS via the lang parameter. **CVE ID : CVE-2021-39368**	N/A	A-CAN-OCE_-020921/75
ced_project					
ced					
Improper Handling of Exceptional Conditions	17-Aug-21	5	ced detects character encoding using Googleâ€™s compact_enc_det library. In ced v0.1.0, passing data types other than `Buffer` causes the Node.js process to crash. The problem has been patched in ced v1.0.0. As a workaround, before passing an argument to ced, verify itâ€™s a `Buffer` using `Buffer.isBuffer(obj)`. **CVE ID : CVE-2021-39131**	https://github.com/sonicdoe/ced/security/advisories/GHSA-27wq-qx3q-fxm9, https://github.com/sonicdoe/ced/commit/a4d9f10b6bf1cd468d1a5b9a283cdf437f8bb7b3	A-CED-CED-020921/76
cerner					
mobile_care					
Improper Neutralization of Special Elements	24-Aug-21	10	A SQL Injection vulnerability in Cerner Mobile Care 5.0.0 allows remote unauthenticated attackers to execute arbitrary	https://www.cerner.com/solutions/mo	A-CER-MOBI-020921/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			SQL commands via a Fullwidth Apostrophe (aka U+FF07) in the default.aspx User ID field. Arbitrary system commands can be executed through the use of xp_cmdshell. **CVE ID : CVE-2021-36385**	bility	
Cisco					
appdynamics_.net_agent					
Improper Privilege Management	18-Aug-21	7.2	A vulnerability in the AppDynamics .NET Agent for Windows could allow an attacker to leverage an authenticated, local user account to gain SYSTEM privileges. This vulnerability is due to the .NET Agent Coordinator Service executing code with SYSTEM privileges. An attacker with local access to a device that is running the vulnerable agent could create a custom process that would be launched with those SYSTEM privileges. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system. This vulnerability is fixed in AppDynamics .NET Agent Release 21.7. **CVE ID : CVE-2021-34745**	https://docs.appdynamics.com/display/PAA/Security+Advisory%3A+AppDynamics+.NET+Agent+Privilege+Escalation+Vulnerability	A-CIS-APPD-020921/78
application_extension_platform					
Improper Input Validation	18-Aug-21	10	A vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	A-CIS-APPL-020921/79

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of incoming UPnP traffic. An attacker could exploit this vulnerability by sending a crafted UPnP request to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a DoS condition. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-34730**	sa-cisco-sb-rv-overflow-htpymMB5	
expressway					
Improper Verification of Cryptographic Signature	18-Aug-21	9	A vulnerability in the image verification function of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker to execute code with internal user privileges on the underlying operating system. The vulnerability is due to insufficient validation of the content of upgrade packages. An attacker could exploit this vulnerability by uploading a malicious archive to the Upgrade page of the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewver-c6WZPXRx	A-CIS-EXPR-020921/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrative web interface. A successful exploit could allow the attacker to execute code with user-level privileges (the _nobody account) on the underlying operating system. **CVE ID : CVE-2021-34715**		
Improper Handling of Exceptional Conditions	18-Aug-21	9	A vulnerability in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker to execute arbitrary code on the underlying operating system as the root user. This vulnerability is due to incorrect handling of certain crafted software images that are uploaded to the affected device. An attacker could exploit this vulnerability by authenticating to the system as an administrative user and then uploading specific crafted software images to the affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID : CVE-2021-34716**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewrce-QPynNCjh	A-CIS-EXPR-020921/81
firepower_management_center					
Exposure of Sensitive Information to an Unauthorize	18-Aug-21	5	A vulnerability in Server Name Identification (SNI) request filtering of Cisco Web Security Appliance (WSA), Cisco Firepower Threat Defense	https://tools.cisco.com/security/center/content/CiscoSecurityAd	A-CIS-FIRE-020921/82

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Actor			(FTD), and the Snort detection engine could allow an unauthenticated, remote attacker to bypass filtering technology on an affected device and exfiltrate data from a compromised host. This vulnerability is due to inadequate filtering of the SSL handshake. An attacker could exploit this vulnerability by using data from the SSL client hello packet to communicate with an external server. A successful exploit could allow the attacker to execute a command-and-control attack on a compromised host and perform additional data exfiltration attacks. **CVE ID : CVE-2021-34749**	visory/cisco-sa-sni-data-exfil-mFgzXqLN	
ironport_web_security_appliance					
Exposure of Sensitive Information to an Unauthorized Actor	18-Aug-21	5	A vulnerability in Server Name Identification (SNI) request filtering of Cisco Web Security Appliance (WSA), Cisco Firepower Threat Defense (FTD), and the Snort detection engine could allow an unauthenticated, remote attacker to bypass filtering technology on an affected device and exfiltrate data from a compromised host. This vulnerability is due to inadequate filtering of the SSL handshake. An attacker could exploit this vulnerability by using data from the SSL client hello packet to communicate	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sni-data-exfil-mFgzXqLN	A-CIS-IRON-020921/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with an external server. A successful exploit could allow the attacker to execute a command-and-control attack on a compromised host and perform additional data exfiltration attacks. **CVE ID : CVE-2021-34749**		
telepresence_video_communication_server					
Improper Verification of Cryptographic Signature	18-Aug-21	9	A vulnerability in the image verification function of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker to execute code with internal user privileges on the underlying operating system. The vulnerability is due to insufficient validation of the content of upgrade packages. An attacker could exploit this vulnerability by uploading a malicious archive to the Upgrade page of the administrative web interface. A successful exploit could allow the attacker to execute code with user-level privileges (the _nobody account) on the underlying operating system. **CVE ID : CVE-2021-34715**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewver-c6WZPXRx	A-CIS-TELE-020921/84
Improper Handling of Exceptional Conditions	18-Aug-21	9	A vulnerability in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	A-CIS-TELE-020921/85

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code on the underlying operating system as the root user. This vulnerability is due to incorrect handling of certain crafted software images that are uploaded to the affected device. An attacker could exploit this vulnerability by authenticating to the system as an administrative user and then uploading specific crafted software images to the affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user. **CVE ID : CVE-2021-34716**	sa-ewrce-QPynNCjh	
Codesys					
codesys					
Deserialization of Untrusted Data	18-Aug-21	6.8	An unsafe deserialization vulnerability exists in the ObjectManager.plugin ObjectStream.ProfileByteArray functionality of CODESYS GmbH CODESYS Development System 3.5.16 and 3.5.17. A specially crafted file can lead to arbitrary command execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21867**	N/A	A-COD-CODE-020921/86
Deserialization of Untrusted Data	18-Aug-21	6.8	An unsafe deserialization vulnerability exists in the ObjectManager.plugin Project.get_MissingTypes()	N/A	A-COD-CODE-020921/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functionality of CODESYS GmbH CODESYS Development System 3.5.16 and 3.5.17. A specially crafted file can lead to arbitrary command execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21868**		
Deserialization of Untrusted Data	25-Aug-21	6.8	An unsafe deserialization vulnerability exists in the Engine.plugin ProfileInformation ProfileData functionality of CODESYS GmbH CODESYS Development System 3.5.16 and 3.5.17. A specially crafted file can lead to arbitrary command execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21869**	N/A	A-COD-CODE-020921/88
compo					
composr_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	In ocProducts Composr CMS before 10.0.38, an attacker can inject JavaScript via Comcode for XSS. **CVE ID : CVE-2021-38708**	https://compo.sr/news/view/announcements/two-new-xss-security.htm	A-COM-COMP-020921/89
Improper Neutralization of Input During Web Page Generation ('Cross-site	16-Aug-21	4.3	In ocProducts Composr CMS before 10.0.38, an attacker can inject JavaScript via the staff_messaging messaging system for XSS. **CVE ID : CVE-2021-38709**	https://compo.sr/news/view/announcements/two-new-xss-security.htm	A-COM-COMP-020921/90

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
contact_form_7_captcha_project					
contact_form_7_captcha					
Cross-Site Request Forgery (CSRF)	23-Aug-21	6.8	The Contact Form 7 Captcha WordPress plugin before 0.0.9 does not have any CSRF check in place when saving its settings, allowing attacker to make a logged in user with the manage_options change them. Furthermore, the settings are not escaped when output in attributes, leading to a Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24565**	https://plugins.trac.wordpress.org/changeset/2570402	A-CON-CONT-020921/91
cozmoslabs					
profile_builder					
Improper Authentication	16-Aug-21	10	The User Registration & User Profile â€“ Profile Builder WordPress plugin before 3.4.9 has a bug allowing any user to reset the password of the admin of the blog, and gain unauthorised access, due to a bypass in the way the reset key is checked. Furthermore, the admin will not be notified of such change by email for example. **CVE ID : CVE-2021-24527**	N/A	A-COZ-PROF-020921/92
crocoblock					
jetengine					
Improper Neutralization of Input During Web Page	16-Aug-21	3.5	Crocoblock JetEngine before 2.6.1 allows XSS by remote authenticated users via a custom form input. **CVE ID : CVE-2021-38607**	https://crocoblock.com/changelog/?plugin=jet-engine	A-CRO-JETE-020921/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')					
current_book_project					
current_book					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	The Current Book WordPress plugin through 1.0.1 does not sanitize user input when an authenticated user adds Author or Book Title, then does not escape these values when outputting to the browser leading to an Authenticated Stored XSS Cross-Site Scripting issue. **CVE ID : CVE-2021-24538**	N/A	A-CUR-CURR-020921/94
custom_login_redirect_project					
custom_login_redirect					
Cross-Site Request Forgery (CSRF)	16-Aug-21	4.3	The Custom Login Redirect WordPress plugin through 1.0.0 does not have CSRF check in place when saving its settings, and do not sanitise or escape user input before outputting them back in the page, leading to a Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24536**	N/A	A-CUS-CUST-020921/95
custom_post_type_relations_project					
custom_post_type_relations					
Improper Neutralization of Input During Web Page Generation ('Cross-site	16-Aug-21	4.3	The Custom Post Type Relations WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the cptr[name] parameter found in the ~/pages/admin-page.php file which allows attackers to	N/A	A-CUS-CUST-020921/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			inject arbitrary web scripts, in versions up to and including 1.0. **CVE ID : CVE-2021-34654**		
cxuu					
cxuucms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	4.3	Multiple Cross Site Scripting (XSS) vulnerabilities exists in CXUUCMS 3.1 in the search and c parameters in (1) public/search.php and in the (2) c parameter in admin.php. **CVE ID : CVE-2021-39599**	N/A	A-CXU-CXUU-020921/97
Cybozu					
garoon					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Aug-21	3.5	Cross-site scripting vulnerability in Scheduler of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20753**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/98
Improper Input Validation	18-Aug-21	4	Improper input validation vulnerability in Workflow of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote authenticated attacker to alter the data of Workflow without the appropriate privilege. **CVE ID : CVE-2021-20754**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/99
Exposure of Resource to Wrong Sphere	18-Aug-21	4	Viewing restrictions bypass vulnerability in Portal of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote authenticated attacker to obtain the data of Portal without the viewing	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege. **CVE ID : CVE-2021-20755**		
Exposure of Resource to Wrong Sphere	18-Aug-21	4	Viewing restrictions bypass vulnerability in Address of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote authenticated attacker to obtain the data of Address without the viewing privilege. **CVE ID : CVE-2021-20756**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/101
Improper Authentication	18-Aug-21	4	Operational restrictions bypass vulnerability in E-mail of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote authenticated attacker to alter the data of Portal without the appropriate privilege. **CVE ID : CVE-2021-20757**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/102
Cross-Site Request Forgery (CSRF)	18-Aug-21	6	Cross-site request forgery (CSRF) vulnerability in Message of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote authenticated attacker to hijack the authentication of administrators and perform an arbitrary operation via unspecified vectors. **CVE ID : CVE-2021-20758**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/103
Improper Authentication	18-Aug-21	4	Operational restrictions bypass vulnerability in Bulletin of Cybozu Garoon 4.6.0 to 5.0.2 allows a remote authenticated attacker to alter the data of Portal without the appropriate privilege. **CVE ID : CVE-2021-20759**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/104
Improper Input	18-Aug-21	4	Improper input validation vulnerability in User Profile of	https://cs.cybozu.co.jp/2	A-CYB-GARO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Cybozu Garoon 4.0.0 to 5.0.2 allows a remote authenticated attacker to alter the data of User Profile without the appropriate privilege. **CVE ID : CVE-2021-20760**	021/007206.html	020921/105
Improper Input Validation	18-Aug-21	3.5	Improper input validation vulnerability in E-mail of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote attacker with an administrative privilege to alter the data of E-mail without the appropriate privilege. **CVE ID : CVE-2021-20761**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/106
Improper Input Validation	18-Aug-21	4	Improper input validation vulnerability in E-mail of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote authenticated to alter the data of E-mail without the appropriate privilege. **CVE ID : CVE-2021-20762**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/107
Exposure of Resource to Wrong Sphere	18-Aug-21	4	Operational restrictions bypass vulnerability in Portal of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote authenticated attacker to obtain the data of Portal without the appropriate privilege. **CVE ID : CVE-2021-20763**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/108
Improper Input Validation	18-Aug-21	5	Improper input validation vulnerability in Attaching Files of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote attacker to alter the data of Attaching Files. **CVE ID : CVE-2021-20764**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/109
Improper	18-Aug-21	4.3	Cross-site scripting	https://cs.cy	A-CYB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			vulnerability in Bulletin of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20765**	bozu.co.jp/2021/007206.html	GARO-020921/110
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Aug-21	4.3	Cross-site scripting vulnerability in Message of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20766**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/111
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Aug-21	3.5	Cross-site scripting vulnerability in Full Text Search of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20767**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/112
Improper Privilege Management	18-Aug-21	4	Operational restrictions bypass vulnerability in Scheduler and MultiReport of Cybozu Garoon 4.0.0 to 5.0.2 allows a remote authenticated attacker to delete the data of Scheduler and MultiReport without the appropriate privilege. **CVE ID : CVE-2021-20768**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/113
Improper Neutralization of Input During Web Page Generation	18-Aug-21	3.5	Cross-site scripting vulnerability in Bulletin of Cybozu Garoon 4.6.0 to 5.0.2 allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2021-20769**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Aug-21	3.5	Cross-site scripting vulnerability in Message of Cybozu Garoon 4.6.0 to 5.0.2 allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20770**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/115
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Aug-21	4.3	Cross-site scripting vulnerability in some functions of Group Mail of Cybozu Garoon 4.0.0 to 5.5.0 allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20771**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/116
Exposure of Sensitive Information to an Unauthorized Actor	18-Aug-21	4	Information disclosure vulnerability in Bulletin of Cybozu Garoon 4.10.0 to 5.5.0 allows a remote authenticated attacker to obtain the title of Bulletin without the viewing privilege. **CVE ID : CVE-2021-20772**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/117
Improper Privilege Management	18-Aug-21	4	There is a vulnerability in Workflow of Cybozu Garoon 4.0.0 to 5.5.0, which may allow a remote authenticated attacker to delete the route information Workflow without the appropriate privilege. **CVE ID : CVE-2021-20773**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/118
Improper Neutralization of Input During Web	18-Aug-21	3.5	Cross-site scripting vulnerability in some functions of E-mail of Cybozu Garoon 4.0.0 to 5.5.0 allows a remote	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20774**		
Improper Input Validation	18-Aug-21	4	Improper input validation vulnerability in Bulletin of Cybozu Garoon 4.10.0 to 5.5.0 allows a remote authenticated attacker to obtain the data of Comment and Space without the viewing privilege. **CVE ID : CVE-2021-20775**	https://cs.cybozu.co.jp/2021/007206.html	A-CYB-GARO-020921/120
digitaldruid					
hoteldruid					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-21	4.3	DigitalDruid HotelDruid 3.0.2 has an XSS vulnerability in prenota.php affecting the fineperiodo1 parameter. **CVE ID : CVE-2021-38559**	N/A	A-DIG-HOTE-020921/121
disc-soft					
daemon_tools					
Out-of-bounds Write	17-Aug-21	7.5	A memory corruption vulnerability exists in the ISO Parsing functionality of Disc Soft Ltd Deamon Tools Pro 8.3.0.0767. A specially crafted malformed file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21832**	N/A	A-DIS-DAEM-020921/122
Dolibarr					
dolibarr					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	17-Aug-21	6.5	In "Dolibarr" application, v3.3.beta1_20121221 to v13.0.2 have "Modify" access for admin level users to change other user's details but fails to validate already existing "Login" name, while renaming the user "Login". This leads to complete account takeover of the victim user. This happens since the password gets overwritten for the victim user having a similar login name. **CVE ID : CVE-2021-25956**	https://github.com/Dolibarr/dolibarr/commit/c4cba43bade736ab89e31013a6ccee59a6e077ee	A-DOL-DOLI-020921/123
Weak Password Recovery Mechanism for Forgotten Password	17-Aug-21	6.5	In "Dolibarr" application, v2.8.1 to v13.0.2 are vulnerable to account takeover via password reset functionality. A low privileged attacker can reset the password of any user in the application using the password reset link the user received through email when requested for a forgotten password. **CVE ID : CVE-2021-25957**	https://github.com/Dolibarr/dolibarr/commit/87f9530272925f0d651f59337a35661faeb6f377	A-DOL-DOLI-020921/124
draftpress					
my_site_audit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	The My Site Audit WordPress plugin through 1.2.4 does not sanitise or escape the Audit Name field when creating an audit, allowing high privilege users to set JavaScript payloads in them, even when he unfiltered_html capability is disallowed, leading to an authenticated Stored Cross-Site Scripting issue	N/A	A-DRA-MY_S-020921/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24445		
Eclipse					
californium					
Improper Verification of Cryptographic Signature	20-Aug-21	5	In Eclipse Californium version 2.0.0 to 2.6.4 and 3.0.0-M1 to 3.0.0-M3, the certificate based (x509 and RPK) DTLS handshakes accidentally succeeds without verifying the server side's signature on the client side, if that signature is not included in the server's ServerKeyExchange. **CVE ID : CVE-2021-34433**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=575281	A-ECL-CALI-020921/126
edit_comments_project					
edit_comments					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-21	7.5	The Edit Comments WordPress plugin through 0.3 does not sanitise, validate or escape the jal_edit_comments GET parameter before using it in a SQL statement, leading to a SQL injection issue **CVE ID : CVE-2021-24551**	N/A	A-EDI-EDIT-020921/127
EDX					
edx-platform					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-21	4.3	Open edX through Lilac.1 allows XSS in common/static/common/js/discussion/utils.js via crafted LaTeX content within a discussion. **CVE ID : CVE-2021-39248**	https://github.com/edx/edx-platform/pull/28379	A-EDX-EDX--020921/128
email-subscriber_project					
email-subscriber					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	4.3	The kento_email_subscriber_ajax AJAX action of the Email Subscriber WordPress plugin through 1.1, does not properly sanitise, validate and escape the submitted subscribe_email and subscribe_name POST parameters, inserting them in the DB and then outputting them back in the Subscriber list (/wp-admin/edit.php?post_type=kes_campaign&page=kento_email_subscriber_list_settings), leading a Stored XSS issue. **CVE ID : CVE-2021-24556**	N/A	A-EMA-EMAI-020921/129
erident_custom_login_and_dashboard_project					
erident_custom_login_and_dashboard					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	3.5	The Erident Custom Login and Dashboard WordPress plugin before 3.5.9 did not properly sanitise its settings, allowing high privilege users to use XSS payloads in them (even when the unfileted_html is disabled) **CVE ID : CVE-2021-24658**	https://plugins.trac.wordpress.org/changeset/2507516	A-ERI-ERID-020921/130
Exponentcms					
exponentcms					
Improper Encoding or Escaping of Output	16-Aug-21	4.3	A HTTP Host header attack exists in ExponentCMS 2.6 and below in /exponent_constants.php. A modified HTTP header can change links on the webpage to an arbitrary value, leading to a possible attack vector for MITM.	N/A	A-EXP-EXPO-020921/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-38751		
expresstech					
quiz_and_survey_master					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Aug-21	4.3	Cross-site scripting vulnerability in Quiz And Survey Master versions prior to 7.1.14 allows a remote attacker to inject arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20792**	https://plugins.trac.wordpress.org/changeset?new=2503364%40quiz-master-next%2Ftrunk%2Fphp%2Fadmin%2Fquizzes-page.php&old=2490516%40quiz-master-next%2Ftrunk%2Fphp%2Fadmin%2Fquizzes-page.php	A-EXP-QUIZ-020921/132
F-secure					
atlant					
N/A	23-Aug-21	4	A Denial-of-Service (DoS) vulnerability was discovered in all versions of F-Secure Atlant whereby the SAVAPI component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33598**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-	A-F-S-ATLA-020921/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				downloads/security-advisories	
elements_endpoint_protection					
N/A	23-Aug-21	4	A Denial-of-Service (DoS) vulnerability was discovered in all versions of F-Secure Atlant whereby the SAVAPI component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33598**	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	A-F-S-ELEM-020921/134
linux_security					
N/A	23-Aug-21	4	A Denial-of-Service (DoS) vulnerability was discovered in all versions of F-Secure Atlant whereby the SAVAPI component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33598**	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	A-F-S-LINU-020921/135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Ffmpeg					
ffmpeg					
Unchecked Return Value	21-Aug-21	7.5	adts_decode_extradata in libavformat/adtsenc.c in FFmpeg 4.4 does not check the init_get_bits return value, which is a necessary step because the second argument to init_get_bits can be crafted. **CVE ID : CVE-2021-38171**	https://github.com/FFmpeg/FFmpeg/commit/9ffa49496d1aae4cbbb387aac28a9e061a6ab0a6, https://patchwork.ffmpeg.org/project/ffmpeg/patch/AS8P193MB12542A86E22F8207EC971930B6F19@AS8P193MB1254.EURP193.PROD.OUTLOOK.COM/	A-FFM-FFMP-020921/136
firefly-iii					
firefly_iii					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-3728**	https://github.com/firefly-iii/firefly-iii/commit/14cdce113e0eb8090d09066fcd2b5cf03b5ac84e, https://hunter.dev/bounties/dd54c5a1-0d4a-4f02-a111-7ce4ddc67a4	A-FIR-FIRE-020921/137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				d	
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-3729**	https://huntr.dev/bounties/d32f3d5a-0738-41ba-89de-34f2a772de76, https://github.com/firefly-iii/firefly-iii/commit/06d319cd71b7787aa919b3ba1ccf51e4ade67712	A-FIR-FIRE-020921/138
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-3730**	https://huntr.dev/bounties/ea181323-51f8-46a2-a60f-6a401907feb7, https://github.com/firefly-iii/firefly-iii/commit/f80178b1b2b7864d17500a131d570c353c9a26f6	A-FIR-FIRE-020921/139
Flatcore					
flatcore-cms					
Improper Neutralization of Input During Web Page Generation	23-Aug-21	3.5	Cross Site Scripting (XSS) vulnerability exiss in FlatCore-CMS 2.0.7 via the upload image function. **CVE ID : CVE-2021-39609**	N/A	A-FLA-FLAT-020921/140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
followistic					
smart_email_alerts					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The Smart Email Alerts WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the api_key in the ~/views/settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.10. **CVE ID : CVE-2021-34642**	N/A	A-FOL-SMAR-020921/141
Fortinet					
fortiportal					
Use of Hard-coded Credentials	18-Aug-21	10	A use of hard-coded credentials (CWE-798) vulnerability in FortiPortal versions 5.2.5 and below, 5.3.5 and below, 6.0.4 and below, versions 5.1.x and 5.0.x may allow a remote and unauthenticated attacker to execute unauthorized commands as root by uploading and deploying malicious web application archive files using the default hard-coded Tomcat Manager username and password. **CVE ID : CVE-2021-32588**	https://fortiguard.com/advisory/FG-IR-21-077	A-FOR-FORT-020921/142
Improper Neutralization of Input During Web Page Generation	19-Aug-21	4.3	An improper neutralization of input during web page generation vulnerability (CWE-79) in FortiPortal GUI 6.0.4 and below, 5.3.6 and below, 5.2.6 and below, 5.1.2 and	https://fortiguard.com/advisory/FG-IR-20-066	A-FOR-FORT-020921/143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			below, 5.0.3 and below, 4.2.2 and below, 4.1.2 and below, 4.0.4 and below may allow a remote and unauthenticated attacker to perform an XSS attack via sending a crafted request with an invalid lang parameter or with an invalid org.springframework.web.servlet.i18n.CookieLocaleResolver.LOCALE value. **CVE ID : CVE-2021-32602**		
freelancetoindia					
paytm-pay					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-21	6.5	The Paytm â€“ Donation Plugin WordPress plugin through 1.3.2 does not sanitise, validate or escape the id GET parameter before using it in a SQL statement when deleting donations, leading to an authenticated SQL injection issue **CVE ID : CVE-2021-24554**	N/A	A-FRE-PAYT-020921/144
Github					
owslib					
Improper Restriction of XML External Entity Reference	23-Aug-21	5	An XML external entity (XXE) injection in PyWPS before 4.5.0 allows an attacker to view files on the application server filesystem by assigning a path to the entity. OWSLib 0.24.1 may also be affected. **CVE ID : CVE-2021-39371**	https://github.com/geopython/pywps/pull/616, https://github.com/geopython/OWSLib/issues/790	A-GIT-OWSL-020921/145
gitit_project					
gitit					
Files or	16-Aug-21	5	In gitit before 0.15.0.0, the	https://githu	A-GIT-GITI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directories Accessible to External Parties			Export feature can be exploited to leak information from files. **CVE ID : CVE-2021-38711**	b.com/jgm/gitit/commit/eed32638f4f6e3b2f4b8a9a04c4b72001acf9ad8, https://github.com/jgm/gitit/compare/0.14.0.0...0.15.0.0	020921/146
Gitlab					
gitlab					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-21	3.5	An issue has been discovered in GitLab affecting all versions starting with 13.3. GitLab was vulnerable to a stored XSS by using the design feature in issues. **CVE ID : CVE-2021-22238**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22238.json	A-GIT-GITL-020921/147
Allocation of Resources Without Limits or Throttling	20-Aug-21	4	A vulnerability was discovered in GitLab versions before 14.0.2, 13.12.6, 13.11.6. GitLab Webhook feature could be abused to perform denial of service attacks. **CVE ID : CVE-2021-22246**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22246.json	A-GIT-GITL-020921/148
Incorrect Authorization	23-Aug-21	5	Improper authorization on the pipelines page in GitLab CE/EE affecting all versions since 13.12 allowed unauthorized users to view some pipeline information for public projects that have access to pipelines restricted to members only **CVE ID : CVE-2021-22248**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22248.json	A-GIT-GITL-020921/149
Generation	23-Aug-21	4	A verbose error message in	https://gitla	A-GIT-GITL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Error Message Containing Sensitive Information			GitLab EE affecting all versions since 12.2 could disclose the private email address of a user invited to a group **CVE ID : CVE-2021-22249**	b.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22249.json	020921/150
Incorrect Authorization	23-Aug-21	4	Improper validation of invited users' email address in GitLab EE affecting all versions since 12.2 allowed projects to add members with email address domain that should be blocked by group settings **CVE ID : CVE-2021-22251**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22251.json, https://gitlab.com/gitlab-org/gitlab/-/issues/14004	A-GIT-GITL-020921/151
Exposure of Resource to Wrong Sphere	23-Aug-21	4	A confusion between tag and branch names in GitLab CE/EE affecting all versions since 13.7 allowed a Developer to access protected CI variables which should only be accessible to Maintainers **CVE ID : CVE-2021-22252**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22252.json	A-GIT-GITL-020921/152
Incorrect Authorization	23-Aug-21	4.9	Improper authorization in GitLab EE affecting all versions since 13.4 allowed a user who previously had the necessary access to trigger deployments to protected environments under specific conditions after the access has been removed **CVE ID : CVE-2021-22253**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22253.json	A-GIT-GITL-020921/153
Improper Encoding or Escaping of Output	20-Aug-21	3.5	Under very specific conditions a user could be impersonated using Gitlab shell. This vulnerability affects GitLab	https://gitlab.com/gitlab-org/cves/-/blob/maste	A-GIT-GITL-020921/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CE/EE 13.1 and later through 14.1.2, 14.0.7 and 13.12.9. **CVE ID : CVE-2021-22254**	r/2021/CVE-2021-22254.json	
givewp					
givewp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	3.5	The GiveWP â€“ Donation Plugin and Fundraising Platform WordPress plugin before 2.12.0 did not escape the Donation Level setting of its Donation Forms, allowing high privilege users to use Cross-Site Scripting payloads in them. **CVE ID : CVE-2021-24524**	N/A	A-GIV-GIVE-020921/155
Gnome					
evolution-rss					
Improper Certificate Validation	22-Aug-21	4.3	In GNOME evolution-rss through 0.3.96, network-soup.c does not enable TLS certificate verification on the SoupSessionSync objects it creates, leaving users vulnerable to network MITM attacks. NOTE: this is similar to CVE-2016-20011. **CVE ID : CVE-2021-39361**	https://gitlab.gnome.org/GNOME/evolution-rss/-/issues/11, https://blogs.gnome.org/mcatanzaro/2021/05/25/reminder-soupsessionsync-and-soupsessionasync-default-to-no-tls-certificate-verification/	A-GNO-EVOL-020921/156
grilo					
Improper Certificate	22-Aug-21	4.3	In GNOME grilo though 0.3.13, grl-net-wc.c does not enable TLS certificate verification on	https://gitlab.gnome.org/GNOME/grilo	A-GNO-GRIL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			the SoupSessionAsync objects it creates, leaving users vulnerable to network MITM attacks. NOTE: this is similar to CVE-2016-20011. **CVE ID : CVE-2021-39365**	/-/issues/146, https://blogs.gnome.org/mcatanzaro/2021/05/25/reminder-soupsessionsync-and-soupsessionasync-default-to-no-tls-certificate-verification/	020921/157
libgda					
Improper Certificate Validation	22-Aug-21	4.3	In GNOME libgda through 6.0.0, gda-web-provider.c does not enable TLS certificate verification on the SoupSessionSync objects it creates, leaving users vulnerable to network MITM attacks. NOTE: this is similar to CVE-2016-20011. **CVE ID : CVE-2021-39359**	https://gitlab.gnome.org/GNOME/libgda/-/issues/249, https://blogs.gnome.org/mcatanzaro/2021/05/25/reminder-soupsessionsync-and-soupsessionasync-default-to-no-tls-certificate-verification/	A-GNO-LIBG-020921/158
libgfbgraph					
Improper Certificate Validation	22-Aug-21	4.3	In GNOME libgfbgraph through 0.2.4, gfbgraph-photo.c does not enable TLS certificate verification on the SoupSessionSync objects it creates, leaving users vulnerable to network MITM	https://gitlab.gnome.org/GNOME/libgfbgraph/-/issues/17, https://blogs.gnome.org/	A-GNO-LIBG-020921/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks. NOTE: this is similar to CVE-2016-20011. **CVE ID : CVE-2021-39358**	mcatanzaro/2021/05/25/reminder-soupsessionsync-and-soupsessionasync-default-to-no-tls-certificate-verification/	
libzapojit					
Improper Certificate Validation	22-Aug-21	4.3	In GNOME libzapojit through 0.0.3, zpj-skydrive.c does not enable TLS certificate verification on the SoupSessionSync objects it creates, leaving users vulnerable to network MITM attacks. NOTE: this is similar to CVE-2016-20011. **CVE ID : CVE-2021-39360**	https://blogs.gnome.org/mcatanzaro/2021/05/25/reminder-soupsessionsync-and-soupsessionasync-default-to-no-tls-certificate-verification/, https://gitlab.gnome.org/GNOME/libzapojit/-/issues/4	A-GNO-LIBZ-020921/160
Google					
chrome					
Out-of-bounds Write	26-Aug-21	6.8	Heap buffer overflow in Bookmarks in Google Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30590**	https://crbug.com/1227777, https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-	A-GOO-CHRO-020921/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				been-updated-to.html	
Use After Free	26-Aug-21	6.8	Use after free in File System API in Google Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30591**	https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html, https://crbug.com/1229298	A-GOO-CHRO-020921/162
Out-of-bounds Write	26-Aug-21	6.8	Out of bounds write in Tab Groups in Google Chrome prior to 92.0.4515.131 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page. **CVE ID : CVE-2021-30592**	https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html, https://crbug.com/1209469	A-GOO-CHRO-020921/163
Out-of-bounds Read	26-Aug-21	5.8	Out of bounds read in Tab Strip in Google Chrome prior to 92.0.4515.131 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted HTML page. **CVE ID : CVE-2021-30593**	https://crbug.com/1209616, https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html	A-GOO-CHRO-020921/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Aug-21	4.6	Use after free in Page Info UI in Google Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via physical access to the device. **CVE ID : CVE-2021-30594**	https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html, https://crbug.com/1218468	A-GOO-CHRO-020921/165
Origin Validation Error	26-Aug-21	4.3	Incorrect security UI in Navigation in Google Chrome on Android prior to 92.0.4515.131 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-30596**	https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html, https://crbug.com/1214481	A-GOO-CHRO-020921/166
Use After Free	26-Aug-21	4.6	Use after free in Browser UI in Google Chrome on Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via physical access to the device. **CVE ID : CVE-2021-30597**	https://crbug.com/1232617, https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html	A-GOO-CHRO-020921/167
Access of Resource Using Incompatible	26-Aug-21	6.8	Type confusion in V8 in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to execute arbitrary code inside a	https://chromereleases.googleblog.com/2021/08/	A-GOO-CHRO-020921/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type ('Type Confusion')			sandbox via a crafted HTML page. **CVE ID : CVE-2021-30598**	stable-channel-update-for-desktop.html, https://crbug.com/1234764	
Access of Resource Using Incompatible Type ('Type Confusion')	26-Aug-21	6.8	Type confusion in V8 in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. **CVE ID : CVE-2021-30599**	https://crbug.com/1234770, https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-020921/169
Use After Free	26-Aug-21	6.8	Use after free in Printing in Google Chrome prior to 92.0.4515.159 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30600**	https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html, https://crbug.com/1231134	A-GOO-CHRO-020921/170
Use After Free	26-Aug-21	6.8	Use after free in Extensions API in Google Chrome prior to 92.0.4515.159 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30601**	https://crbug.com/1234009, https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-020921/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Aug-21	6.8	Use after free in WebRTC in Google Chrome prior to 92.0.4515.159 allowed an attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30602**	https://crbug.com/1230767, https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-020921/172
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	26-Aug-21	5.1	Data race in WebAudio in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30603**	https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html, https://crbug.com/1233564	A-GOO-CHRO-020921/173
Use After Free	26-Aug-21	6.8	Use after free in ANGLE in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30604**	https://crbug.com/1234829, https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-020921/174
gpac					
gpac					
Integer Overflow or Wraparound	25-Aug-21	6.8	An exploitable integer overflow vulnerability exists within the MPEG-4 decoding functionality of the GPAC	N/A	A-GPA-GPAC-020921/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input when decoding the atom for the "co64" FOURCC can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21834**		
Integer Overflow or Wraparound	25-Aug-21	6.8	An exploitable integer overflow vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input when decoding the atom associated with the "csgp" FOURCC can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21835**	N/A	A-GPA-GPAC-020921/176
Integer Overflow or Wraparound	25-Aug-21	6.8	An exploitable integer overflow vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input using the "ctts" FOURCC code can cause an integer overflow due to	N/A	A-GPA-GPAC-020921/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21836**		
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21837**	N/A	A-GPA-GPAC-020921/178
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21838**	N/A	A-GPA-GPAC-020921/179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21839**	N/A	A-GPA-GPAC-020921/180
Integer Overflow or Wraparound	25-Aug-21	6.8	An exploitable integer overflow vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input used to process an atom using the "saio" FOURCC code cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21840**	N/A	A-GPA-GPAC-020921/181
Integer Overflow or Wraparound	25-Aug-21	6.8	An exploitable integer overflow vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input when	N/A	A-GPA-GPAC-020921/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reading an atom using the 'sbgp' FOURCC code can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21841**		
Integer Overflow or Wraparound	25-Aug-21	6.8	An exploitable integer overflow vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow when processing an atom using the 'ssix' FOURCC code, due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21842**	N/A	A-GPA-GPAC-020921/183
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. After	N/A	A-GPA-GPAC-020921/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validating the number of ranges, at [41] the library will multiply the count by the size of the GF_SubsegmentRangeInfo structure. On a 32-bit platform, this multiplication can result in an integer overflow causing the space of the array being allocated to be less than expected. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21843**		
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input when encountering an atom using the “stco” FOURCC code, can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21844**	N/A	A-GPA-GPAC-020921/185
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input in “stsc” decoder can cause an integer	N/A	A-GPA-GPAC-020921/186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21845**		
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input in "stsz" decoder can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21846**	N/A	A-GPA-GPAC-020921/187
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input in "stts" decoder can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability.	N/A	A-GPA-GPAC-020921/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21847		
Integer Overflow or Wraparound	25-Aug-21	6.8	An exploitable integer overflow vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. The library will actually reuse the parser for atoms with the "stsz" FOURCC code when parsing atoms that use the "stz2" FOURCC code and can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21848**	N/A	A-GPA-GPAC-020921/189
Integer Overflow or Wraparound	25-Aug-21	6.8	An exploitable integer overflow vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow when the library encounters an atom using the "tfra" FOURCC code due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21849**	N/A	A-GPA-GPAC-020921/190
Integer	25-Aug-21	6.8	An exploitable integer	N/A	A-GPA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			overflow vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow when the library encounters an atom using the "trun" FOURCC code due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21850**		GPAC-020921/191
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input at "csgp" decoder sample group description indices can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21851**	N/A	A-GPA-GPAC-020921/192
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially	N/A	A-GPA-GPAC-020921/193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted MPEG-4 input at "stss" decoder can cause an integer overflow due to unchecked arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21852**		
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow due to unchecked addition arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21853**	N/A	A-GPA-GPAC-020921/194
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow due to unchecked addition arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this	N/A	A-GPA-GPAC-020921/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. **CVE ID : CVE-2021-21854**		
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow due to unchecked addition arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21855**	N/A	A-GPA-GPAC-020921/196
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow due to unchecked addition arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21856**	N/A	A-GPA-GPAC-020921/197
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content	N/A	A-GPA-GPAC-020921/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow due to unchecked addition arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21857**		
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an integer overflow due to unchecked addition arithmetic resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21858**	N/A	A-GPA-GPAC-020921/199
Integer Overflow or Wraparound	16-Aug-21	6.8	An exploitable integer truncation vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. The stri_box_read function is used when processing atoms using the 'stri' FOURCC code. An attacker can convince a user to open a video to trigger this vulnerability.	N/A	A-GPA-GPAC-020921/200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21859		
Allocation of Resources Without Limits or Throttling	16-Aug-21	6.8	An exploitable integer truncation vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially crafted MPEG-4 input can cause an improper memory allocation resulting in a heap-based buffer overflow that causes memory corruption. The FOURCC code, 'trik', is parsed by the function within the library. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21860**	N/A	A-GPA-GPAC-020921/201
Allocation of Resources Without Limits or Throttling	16-Aug-21	6.8	An exploitable integer truncation vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. When processing the 'hdlr' FOURCC code, a specially crafted MPEG-4 input can cause an improper memory allocation resulting in a heap-based buffer overflow that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21861**	N/A	A-GPA-GPAC-020921/202
Integer Overflow or Wraparound	18-Aug-21	6.8	Multiple exploitable integer truncation vulnerabilities exist within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content	N/A	A-GPA-GPAC-020921/203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			library v1.0.1. A specially crafted MPEG-4 input can cause an improper memory allocation resulting in a heap-based buffer overflow that causes memory corruption The implementation of the parser used for the "Xtra" FOURCC code is handled. An attacker can convince a user to open a video to trigger this vulnerability. **CVE ID : CVE-2021-21862**		
haikuforteams					
diez					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Aug-21	6.8	The @diez/generation npm package is a client for Diez. The locateFont method of @diez/generation has a command injection vulnerability. Clients of the @diez/generation library are unlikely to be aware of this, so they might unwittingly write code that contains a vulnerability. This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. All versions of this package are vulnerable as of the writing of this CVE. **CVE ID : CVE-2021-32830**	https://securitylab.github.com/advisories/GHSL-2021-061-diez-generation-cmd-injection/	A-HAI-DIEZ-020921/204
Haproxy					
haproxy					
N/A	17-Aug-21	5	An issue was discovered in HAProxy 2.2 before 2.2.16, 2.3 before 2.3.13, and 2.4 before	https://git.haproxy.org/?p=haproxy.git;	A-HAP-HAPR-020921/205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.4.3. It does not ensure that the scheme and path portions of a URI have the expected characters. For example, the authority field (as observed on a target HTTP/2 server) might differ from what the routing rules were intended to achieve. **CVE ID : CVE-2021-39240**	a=commit;h=a495e0d94876c9d39763db319f609351907a31e8, https://git.haproxy.org/?p=haproxy.git;a=commit;h=4b8852c70d8c4b7e225e24eb58258a15eb54c26e	
N/A	17-Aug-21	5	An issue was discovered in HAProxy 2.0 before 2.0.24, 2.2 before 2.2.16, 2.3 before 2.3.13, and 2.4 before 2.4.3. An HTTP method name may contain a space followed by the name of a protected resource. It is possible that a server would interpret this as a request for that protected resource, such as in the "GET /admin? HTTP/1.1 /static/images HTTP/1.1" example. **CVE ID : CVE-2021-39241**	https://git.haproxy.org/?p=haproxy.git;a=commit;h=89265224d314a056d77d974284802c1b8a0dc97f	A-HAP-HAPR-020921/206
Improper Handling of Exceptional Conditions	17-Aug-21	5	An issue was discovered in HAProxy 2.2 before 2.2.16, 2.3 before 2.3.13, and 2.4 before 2.4.3. It can lead to a situation with an attacker-controlled HTTP Host header, because a mismatch between Host and authority is mishandled. **CVE ID : CVE-2021-39242**	https://git.haproxy.org/?p=haproxy.git;a=commit;h=b5d2b9e154d78e4075db163826c5e0f6d31b2ab1	A-HAP-HAPR-020921/207
harmonicdesign					
hd_quiz					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	3.5	The HD Quiz WordPress plugin before 1.8.4 does not escape some of its Answers before outputting them in attribute when generating the Quiz, which could lead to Stored Cross-Site Scripting issues **CVE ID : CVE-2021-24571**	N/A	A-HAR-HD_Q-020921/208
hbs_project					
hbs					
Exposure of Sensitive Information to an Unauthorized Actor	16-Aug-21	5	The npm hbs package is an Express view engine wrapper for Handlebars. Depending on usage, users of hbs may be vulnerable to a file disclosure vulnerability. There is currently no patch for this vulnerability. hbs mixes pure template data with engine configuration options through the Express render API. By overwriting internal configuration options a file disclosure vulnerability may be triggered in downstream applications. For an example PoC see the referenced GHSL-2021-020. **CVE ID : CVE-2021-32822**	https://securitylab.github.com/advisories/GHSL-2021-020-pillarjs-hbs/	A-HBS-HBS-020921/209
hcc-embedded					
interniche					
Out-of-bounds Write	19-Aug-21	7.5	An issue was discovered in HCC embedded InterNiche 4.0.1. A potential heap buffer overflow exists in the code that parses the HTTP POST request, due to lack of size validation. This vulnerability requires the	N/A	A-HCC-INTE-020921/210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to send a crafted HTTP POST request with a URI longer than 50 bytes. This leads to a heap overflow in wbs_post() via an strcpy() call. **CVE ID : CVE-2021-31226**		
nichestack					
Loop with Unreachable Exit Condition ('Infinite Loop')	19-Aug-21	5	The web server in InterNiche NicheStack through 4.0.1 allows remote attackers to cause a denial of service (infinite loop and networking outage) via an unexpected valid HTTP request such as OPTIONS. This occurs because the HTTP request handler enters a miscoded wbs_loop() debugger hook. **CVE ID : CVE-2021-27565**	N/A	A-HCC-NICH-020921/211
Out-of-bounds Write	19-Aug-21	5	An issue was discovered in HCC embedded InterNiche 4.0.1. A potential heap buffer overflow exists in the code that parses the HTTP POST request, due to an incorrect signed integer comparison. This vulnerability requires the attacker to send a malformed HTTP packet with a negative Content-Length, which bypasses the size checks and results in a large heap overflow in the wbs_multidata buffer copy. **CVE ID : CVE-2021-31227**	N/A	A-HCC-NICH-020921/212
Insufficient Verification of Data Authenticity	19-Aug-21	5	An issue was discovered in HCC embedded InterNiche 4.0.1. This vulnerability allows the attacker to predict a DNS	N/A	A-HCC-NICH-020921/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			query's source port in order to send forged DNS response packets that will be accepted as valid answers to the DNS client's requests (without sniffing the specific request). Data is predictable because it is based on the time of day, and has too few bits. **CVE ID : CVE-2021-31228**		
Loop with Unreachable Exit Condition ('Infinite Loop')	19-Aug-21	5	An issue was discovered in tcp_pulloutofband() in tcp_in.c in HCC embedded InterNiche 4.0.1. The TCP out-of-band urgent-data processing function invokes a panic function if the pointer to the end of the out-of-band data points outside of the TCP segment's data. If the panic function hadn't a trap invocation removed, it will enter an infinite loop and therefore cause DoS (continuous loop or a device reset). **CVE ID : CVE-2021-31400**	N/A	A-HCC-NICH-020921/214
Improper Input Validation	19-Aug-21	5	An issue was discovered in tcp_rcv() in nptcp.c in HCC embedded InterNiche 4.0.1. The TCP header processing code doesn't sanitize the value of the IP total length field (header length + data length). With a crafted IP packet, an integer overflow occurs whenever the value of the IP data length is calculated by subtracting the length of the header from the total length of	https://cert-portal.siemens.com/productcert/pdf/ssa-789208.pdf	A-HCC-NICH-020921/215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the IP packet. **CVE ID : CVE-2021-31401**		
Improper Check for Dropped Privileges	19-Aug-21	7.8	An issue was discovered in HCC Embedded InterNiche NicheStack through 4.3. The tfshnd():tftpsrv.c TFTP packet processing function doesn't ensure that a filename is adequately '\0' terminated; therefore, a subsequent call to strlen for the filename might read out of bounds of the protocol packet buffer (if no '\0' byte exists within a reasonable range). **CVE ID : CVE-2021-36762**	N/A	A-HCC-NICH-020921/216
hitachiabb-powergrids					
counterparty_settlement_and_billing					
Insufficiently Protected Credentials	20-Aug-21	6.5	Insufficiently Protected Credentials vulnerability in client environment of Hitachi ABB Power Grids Retail Operations and Counterparty Settlement Billing (CSB) allows an attacker or unauthorized user to access database credentials, shut down the product and access or alter. This issue affects: Hitachi ABB Power Grids Retail Operations version 5.7.2 and prior versions. Hitachi ABB Power Grids Counterparty Settlement Billing (CSB) version 5.7.2 and prior versions. **CVE ID : CVE-2021-35529**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK107992A5821&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=9AKK107992A5933&LanguageCode=en&DocumentPartId=&Action	A-HIT-COUN-020921/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				=Launch	
retail_operations					
Insufficiently Protected Credentials	20-Aug-21	6.5	Insufficiently Protected Credentials vulnerability in client environment of Hitachi ABB Power Grids Retail Operations and Counterparty Settlement Billing (CSB) allows an attacker or unauthorized user to access database credentials, shut down the product and access or alter. This issue affects: Hitachi ABB Power Grids Retail Operations version 5.7.2 and prior versions. Hitachi ABB Power Grids Counterparty Settlement Billing (CSB) version 5.7.2 and prior versions. **CVE ID : CVE-2021-35529**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK107992A5821&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=9AKK107992A5933&LanguageCode=en&DocumentPartId=&Action=Launch	A-HIT-RETA-020921/218
hmplugin					
hm_multiple_roles					
Improper Privilege Management	23-Aug-21	6.5	The HM Multiple Roles WordPress plugin before 1.3 does not have any access control to prevent low privilege users to set themselves as admin via their profile page **CVE ID : CVE-2021-24602**	N/A	A-HMP-HM_M-020921/219
hornerautomation					
cscape					
Out-of-bounds Read	25-Aug-21	6.8	Cscape (All Versions prior to 9.90 SP5) lacks proper	N/A	A-HOR-CSCA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied data when parsing project files. This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2021-32975**		020921/220
hospital_management_system_project					
hospital_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Aug-21	7.5	SQL Injection vulnerability in Hospital Management System due to lack of input validation in messearch.php. **CVE ID : CVE-2021-38754**	N/A	A-HOS-HOSP-020921/221
Missing Authorization	16-Aug-21	5	Unauthenticated doctor entry deletion in Hospital Management System in admin-panel1.php. **CVE ID : CVE-2021-38755**	N/A	A-HOS-HOSP-020921/222
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	Persistent cross-site scripting (XSS) in Hospital Management System targeted towards web admin through prescribe.php. **CVE ID : CVE-2021-38756**	N/A	A-HOS-HOSP-020921/223
Improper Neutralization of Input During Web Page Generation	16-Aug-21	4.3	Persistent cross-site scripting (XSS) in Hospital Management System targeted towards web admin through contact.php. **CVE ID : CVE-2021-38757**	N/A	A-HOS-HOSP-020921/224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Huawei					
elf-g10hn					
Improper Privilege Management	23-Aug-21	5	There is a logic vulnerability in Elf-G10HN 1.0.0.608. An unauthenticated attacker could perform specific operations to exploit this vulnerability. Due to insufficient security design, successful exploit could allow an attacker to add users to be friends without prompting in the target device. **CVE ID : CVE-2021-22449**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210630-01-logic-en	A-HUA-ELF--020921/225
IBM					
resilient_security_orchestration_automation_and_response					
Use of a Broken or Risky Cryptographic Algorithm	23-Aug-21	5	IBM Security SOAR uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID : CVE-2021-29704**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200660, https://www.ibm.com/support/pages/node/6482585	A-IBM-RESI-020921/226
Improper Privilege Management	23-Aug-21	5	IBM Security SOAR performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses. **CVE ID : CVE-2021-29802**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204059, https://www.ibm.com/support/pages/node/6482689	A-IBM-RESI-020921/227
Icinga					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
icinga					
Improper Certificate Validation	19-Aug-21	5	Icinga is a monitoring system which checks the availability of network resources, notifies users of outages, and generates performance data for reporting. In versions 2.5.0 through 2.13.0, ElasticsearchWriter, GelfWriter, InfluxdbWriter and Influxdb2Writer do not verify the server's certificate despite a certificate authority being specified. Icinga 2 instances which connect to any of the mentioned time series databases (TSDBs) using TLS over a spoofable infrastructure should immediately upgrade to version 2.13.1, 2.12.6, or 2.11.11 to patch the issue. Such instances should also change the credentials (if any) used by the TSDB writer feature to authenticate against the TSDB. There are no workarounds aside from upgrading. **CVE ID : CVE-2021-37698**	https://github.com/Icinga/icinga2/security/advisories/GHSA-cxfm-8j5v-5qr2	A-ICI-ICIN-020921/228
imgurl_project					
imgurl					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	imgURL 2.31 allows XSS via an X-Forwarded-For HTTP header. **CVE ID : CVE-2021-38713**	N/A	A-IMG-IMGU-020921/229
invisioncommunity					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
invision_power_board					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-21	3.5	Invision Community (aka IPS Community Suite or IP-Board) before 4.6.5.1 allows reflected XSS because the filenames of uploaded files become predictable through a brute-force attack against the PHP mt_rand function. **CVE ID : CVE-2021-39249**	https://invisioncommunity.com/release-notes/4651-r102/	A-INV-INVI-020921/230
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-21	3.5	Invision Community (aka IPS Community Suite or IP-Board) before 4.6.5.1 allows stored XSS, with resultant code execution, because an uploaded file can be placed in an IFRAME element within user-generated content. For code execution, the attacker can rely on the ability of an admin to install widgets, disclosure of the admin session ID in a Referer header, and the ability of an admin to use the templating engine (e.g., Edit HTML). **CVE ID : CVE-2021-39250**	https://invisioncommunity.com/release-notes/4651-r102/	A-INV-INVI-020921/231
ISC					
bind					
Reachable Assertion	18-Aug-21	5	In BIND 9.16.19, 9.17.16. Also, version 9.16.19-S1 of BIND Supported Preview Edition When a vulnerable version of named receives a query under the circumstances described above, the named process will terminate due to a failed assertion check. The vulnerability affects only BIND	https://kb.isc.org/v1/docs/cve-2021-25218, http://www.openwall.com/lists/oss-security/2021/08/18/3, http://www.	A-ISC-BIND-020921/232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9 releases 9.16.19, 9.17.16, and release 9.16.19-S1 of the BIND Supported Preview Edition. **CVE ID : CVE-2021-25218**	openwall.com/lists/oss-security/2021/08/20/2	
Joomla					
joomla\\!					
Incorrect Authorization	24-Aug-21	6.4	An issue was discovered in Joomla! 4.0.0. The media manager does not correctly check the user's permissions before executing a file deletion command. **CVE ID : CVE-2021-26040**	https://developer.joomla.org/security-centre/861-20210801-core-insufficient-access-control-for-com-media-deletion-endpoint	A-JOO-JOOM-020921/233
joplinapp					
joplin					
Cross-Site Request Forgery (CSRF)	24-Aug-21	6.8	The package joplin before 2.3.2 are vulnerable to Cross-site Request Forgery (CSRF) due to missing CSRF checks in various forms. **CVE ID : CVE-2021-23431**	https://github.com/laurent22/joplin/commit/19b45de2981c09f6f387498ef96d32b4811eba5e, https://snyk.io/vuln/SNYK-JS-JOPLIN-1325537	A-JOP-JOPL-020921/234
jsoup					
jsoup					
Uncaught Exception	18-Aug-21	5	jsoup is a Java library for working with HTML. Those using jsoup versions prior to 1.14.2 to parse untrusted	https://jsoup.org/news/release-1.14.1, https://jsoup	A-JSO-JSOU-020921/235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML or XML may be vulnerable to DOS attacks. If the parser is run on user supplied input, an attacker may supply content that causes the parser to get stuck (loop indefinitely until cancelled), to complete more slowly than usual, or to throw an unexpected exception. This effect may support a denial of service attack. The issue is patched in version 1.14.2. There are a few available workarounds. Users may rate limit input parsing, limit the size of inputs based on system resources, and/or implement thread watchdogs to cap and timeout parse runtimes. **CVE ID : CVE-2021-37714**	.org/news/release-1.14.2, https://github.com/jhy/jsoup/security/advisories/GHSA-m72m-mhq2-9p6c	
jupyterhub					
nbgitpuller					
Improper Control of Generation of Code ('Code Injection')	25-Aug-21	6.8	nbgitpuller is a Jupyter server extension to sync a git repository one-way to a local path. Due to unsanitized input, visiting maliciously crafted links could result in arbitrary code execution in the user environment. This has been resolved in version 0.10.2 and all users are advised to upgrade. No work around exist for users who can not upgrade. **CVE ID : CVE-2021-39160**	https://github.com/jupyterhub/nbgitpuller/security/advisories/GHSA-mq5p-2mcr-m52j, https://github.com/jupyterhub/nbgitpuller/commit/07690644f29a566011dd0d7ba14cae3eb0490481	A-JUP-NBGI-020921/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
keszites					
simple_popup_newsletter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The Simple Popup Newsletter WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of $_SERVER['PHP_SELF'] in the ~/simple-popup-newsletter.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.4.7. **CVE ID : CVE-2021-34658**	N/A	A-KES-SIMP-020921/237
kn_fix_your_title_project					
kn_fix_your_title					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	3.5	The KN Fix Your Title WordPress plugin through 1.0.1 was vulnerable to Authenticated Stored XSS in the separator field. **CVE ID : CVE-2021-24547**	N/A	A-KN_-KN_F-020921/238
komoot					
komoot					
Exposure of Sensitive Information to an Unauthorized Actor	20-Aug-21	5	An information disclosure vulnerability exists in the Friend finder functionality of GmbH Komoot version 10.26.9 up to 11.1.11. A specially crafted series of network requests can lead to the disclosure of sensitive information. **CVE ID : CVE-2021-21823**	N/A	A-KOM-KOMO-020921/239
Ledgersmb					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ledgersmb					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	6.8	LedgerSMB does not check the origin of HTML fragments merged into the browser's DOM. By sending a specially crafted URL to an authenticated user, this flaw can be abused for remote code execution and information disclosure. **CVE ID : CVE-2021-3693**	https://ledgersmb.org/cve-2021-3693-cross-site-scripting, https://huntr.dev/bounties/daf1384d-648a-43fd-9b35-5c37d8ead667	A-LED-LEDG-020921/240
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	6.8	LedgerSMB does not sufficiently HTML-encode error messages sent to the browser. By sending a specially crafted URL to an authenticated user, this flaw can be abused for remote code execution and information disclosure. **CVE ID : CVE-2021-3694**	https://huntr.dev/bounties/ef7f4cf7-3a81-4516-b261-f5b6ac21430c, https://ledgersmb.org/cve-2021-3694-cross-site-scripting, https://github.com/ledgersmb/ledgersmb/commit/98fa476d46a4a7e5e9492ed69b4fa190be5547fc	A-LED-LEDG-020921/241
Improper Restriction of Rendered UI Layers or Frames	23-Aug-21	4.3	LedgerSMB does not sufficiently guard against being wrapped by other sites, making it vulnerable to 'clickjacking'. This allows an attacker to trick a targetted user to execute unintended	https://huntr.dev/bounties/5664331d-f5f8-4412-8566-408f8655888a,	A-LED-LEDG-020921/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			actions. **CVE ID : CVE-2021-3731**	https://ledgersmb.org/cve-2021-3731-clickjacking	
Lenovo					
drivers_management					
Untrusted Search Path	17-Aug-21	6.9	A DLL preloading vulnerability was reported in Lenovo Driver Management prior to version 2.9.0719.1104 that could allow privilege escalation. **CVE ID : CVE-2021-3633**	https://iknow.lenovo.com.cn/detail/dc_198418.html	A-LEN-DRIV-020921/243
lifterlms					
lifterlms					
Authorization Bypass Through User-Controlled Key	23-Aug-21	5	The LMS by LifterLMS â€“ Online Course, Membership & Learning Management System Plugin for WordPress plugin before 4.21.2 was affected by an IDOR issue, allowing students to see other student answers and grades **CVE ID : CVE-2021-24562**	https://make.lifterlms.com/2021/05/17/lifterlms-version-4-21-2/	A-LIF-LIFT-020921/244
light_messages_project					
light_messages					
Cross-Site Request Forgery (CSRF)	16-Aug-21	4.3	The Light Messages WordPress plugin through 1.0 is lacking CSRF check when updating it's settings, and is not sanitising its Message Content in them (even with the unfiltered_html disallowed). As a result, an attacker could make a logged in admin update the settings to arbitrary values, and set a Cross-Site Scripting payload in the Message Content.	N/A	A-LIG-LIGH-020921/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Depending on the options set, the XSS payload can be triggered either in the backend only (in the plugin's settings), or both frontend and backend. **CVE ID : CVE-2021-24535**		
Live555					
live555					
Missing Release of Resource after Effective Lifetime	18-Aug-21	5	Live555 through 1.08 has a memory leak in AC3AudioStreamParser for AC3 files. **CVE ID : CVE-2021-39282**	http://www.live555.com/liveMedia/public/changelog.txt#[2021.08.13], http://lists.live555.com/pipermail/live-devel/2021-August/021970.html	A-LIV-LIVE-020921/246
Reachable Assertion	18-Aug-21	4.3	liveMedia/FramedSource.cpp in Live555 through 1.08 allows an assertion failure and application exit via multiple SETUP and PLAY commands. **CVE ID : CVE-2021-39283**	http://www.live555.com/liveMedia/public/changelog.txt#[2021.08.13], http://lists.live555.com/pipermail/live-devel/2021-August/021969.html	A-LIV-LIVE-020921/247
local_services_search_engine_management_system_project					
local_services_search_engine_management_system					
Improper Neutralization of Special Elements	19-Aug-21	4	A SQL injection vulnerability was discovered in the editid parameter in Local Services Search Engine Management	N/A	A-LOC-LOCA-020921/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			System Project 1.0. This vulnerability gives admin users the ability to dump all data from the database. **CVE ID : CVE-2021-27999**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Aug-21	3.5	A persistent cross-site scripting vulnerability was discovered in Local Services Search Engine Management System Project 1.0 which allows remote attackers to execute arbitrary code via crafted payloads entered into the Name and Address fields. **CVE ID : CVE-2021-28000**	N/A	A-LOC-LOCA-020921/249
meowapps					
media_usage					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The Media Usage WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the id parameter in the ~/mmu_admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.0.4. **CVE ID : CVE-2021-34652**	N/A	A-MEO-MEDI-020921/250
mimetic					
mimetic_books					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	The Mimetic Books WordPress plugin through 0.2.13 was vulnerable to Authenticated Stored Cross-Site Scripting (XSS) in the "Default Publisher ID" field on the plugin's settings page. **CVE ID : CVE-2021-24548**	N/A	A-MIM-MIME-020921/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
miniftpd_project					
miniftpd					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Aug-21	4	A Buffer Overflow vulnerabilty exists in Miniftpd 1.0 in the do_mkd function in the ftpproto.c file, which could let a remote malicious user cause a Denial of Service. **CVE ID : CVE-2021-39602**	N/A	A-MIN-MINI-020921/252
Misp					
misp					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Aug-21	6.8	MISP 2.4.148, in certain configurations, allows SQL injection via the app/Model/Log.php $conditions['org'] value. **CVE ID : CVE-2021-39302**	https://github.com/MISP/MISP/commit/20d9020b76d1f6790c4d84e020d0cc97c929f66b	A-MIS-MISP-020921/253
MIT					
kerberos_5					
NULL Pointer Dereference	23-Aug-21	4	The Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.18.5 and 1.19.x before 1.19.3 has a NULL pointer dereference in kdc/do_tgs_req.c via a FAST inner body that lacks a server field. **CVE ID : CVE-2021-37750**	https://web.mit.edu/kerberos/advisories/, https://github.com/krb5/krb5/commit/d775c95af7606a51bf79547a94fa52ddd1cb7f49	A-MIT-KERB-020921/254
mock-server					
mockserver					
Improper Neutralizatio	16-Aug-21	6.8	MockServer is open source software which enables easy	https://securitylab.github.	A-MOC-MOCK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements in Output Used by a Downstream Component ('Injection')			mocking of any system you integrate with via HTTP or HTTPS. An attacker that can trick a victim into visiting a malicious site while running MockServer locally, will be able to run arbitrary code on the MockServer machine. With an overly broad default CORS configuration MockServer allows any site to send cross-site requests. Additionally, MockServer allows you to create dynamic expectations using Javascript or Velocity templates. Both engines may allow an attacker to execute arbitrary code on-behalf of MockServer. By combining these two issues (Overly broad CORS configuration + Script injection), an attacker could serve a malicious page so that if a developer running MockServer visits it, they will get compromised. For more details including a PoC see the referenced GHSL-2021-059. **CVE ID : CVE-2021-32827**	com/advisories/GHSL-2021-059-mockserver/	020921/255
mootools_project					
mootools					
N/A	24-Aug-21	7.5	This affects all versions of package mootools. This is due to the ability to pass untrusted input to Object.merge() **CVE ID : CVE-2021-23432**	N/A	A-MOO-MOOT-020921/256
moova					
moova_for_woocommerce					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The Moova for WooCommerce WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the lat parameter in the ~/Checkout/Checkout.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.5. **CVE ID : CVE-2021-34664**	N/A	A-MOO-MOOV-020921/257
Mozilla					
firefox					
Missing Initialization of Resource	17-Aug-21	6.8	Uninitialized memory in a canvas object could have caused an incorrect free() leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29980**	https://bugzilla.mozilla.org/show_bug.cgi?id=1722204, https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/	A-MOZ-FIRE-020921/258
N/A	17-Aug-21	6.8	An issue present in lowering/register allocation could have led to obscure but deterministic register confusion failures in JITted code that would lead to a	https://bugzilla.mozilla.org/show_bug.cgi?id=1707774, https://www	A-MOZ-FIRE-020921/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially exploitable crash. This vulnerability affects Firefox < 91 and Thunderbird < 91. **CVE ID : CVE-2021-29981**	.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/	
Missing Release of Resource after Effective Lifetime	17-Aug-21	4.3	Due to incorrect JIT optimization, we incorrectly interpreted data from the wrong type of object, resulting in the potential leak of a single bit of memory. This vulnerability affects Firefox < 91 and Thunderbird < 91. **CVE ID : CVE-2021-29982**	https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://bugzilla.mozilla.org/show_bug.cgi?id=1715318	A-MOZ-FIRE-020921/260
N/A	17-Aug-21	4.3	Firefox for Android could get stuck in fullscreen mode and not exit it even after normal interactions that should cause it to exit. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 91. **CVE ID : CVE-2021-29983**	https://www.mozilla.org/security/advisories/mfsa2021-33/, https://bugzilla.mozilla.org/show_bug.cgi?id=1719088	A-MOZ-FIRE-020921/261
N/A	17-Aug-21	6.8	Instruction reordering resulted in a sequence of instructions that would cause an object to be incorrectly considered during garbage collection. This led to memory	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www	A-MOZ-FIRE-020921/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29984**	.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://www.mozilla.org/security/advisories/mfsa2021-35/	
Use After Free	17-Aug-21	6.8	A use-after-free vulnerability in media channels could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29985**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://www.mozilla.org/security/advisories/mfsa2021-35/	A-MOZ-FIRE-020921/263
Concurrent Execution using Shared Resource with Improper	17-Aug-21	6.8	A suspected race condition when calling getaddrinfo led to memory corruption and a potentially exploitable crash. *Note: This issue only affected Linux operating systems. Other	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www	A-MOZ-FIRE-020921/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			operating systems are unaffected.* This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29986**	.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://www.mozilla.org/security/advisories/mfsa2021-35/	
Improper Restriction of Excessive Authentication Attempts	17-Aug-21	4.3	After requesting multiple permissions, and closing the first permission panel, subsequent permission panels will be displayed in a different position but still record a click in the default location, making it possible to trick a user into accepting a permission they did not want to. *This bug only affects Firefox on Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox < 91 and Thunderbird < 91. **CVE ID : CVE-2021-29987**	https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://bugzilla.mozilla.org/show_bug.cgi?id=1716129	A-MOZ-FIRE-020921/265
Interpretation Conflict	17-Aug-21	6.8	Firefox incorrectly treated an inline list-item element as a block element, resulting in an out of bounds read or memory corruption, and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/,	A-MOZ-FIRE-020921/266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29988	https://www.mozilla.org/security/advisories/mfsa2021-36/, https://www.mozilla.org/security/advisories/mfsa2021-35/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 90 and Firefox ESR 78.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.13, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29989**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-35/	A-MOZ-FIRE-020921/267
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-21	6.8	Mozilla developers and community members reported memory safety bugs present in Firefox 90. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 91. **CVE ID : CVE-2021-29990**	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1544190%2C1716481%2C1717778%2C1719319%2C1722073, https://www.mozilla.org/security/advisories/mfsa2021-33/	A-MOZ-FIRE-020921/268
firefox_esr					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Initialization of Resource	17-Aug-21	6.8	Uninitialized memory in a canvas object could have caused an incorrect free() leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29980**	https://bugzilla.mozilla.org/show_bug.cgi?id=1722204, https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/	A-MOZ-FIRE-020921/269
N/A	17-Aug-21	6.8	Instruction reordering resulted in a sequence of instructions that would cause an object to be incorrectly considered during garbage collection. This led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29984**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://www.mozilla.org/security/advisories/mfsa2021-35/	A-MOZ-FIRE-020921/270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Aug-21	6.8	A use-after-free vulnerability in media channels could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29985**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://www.mozilla.org/security/advisories/mfsa2021-35/	A-MOZ-FIRE-020921/271
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Aug-21	6.8	A suspected race condition when calling getaddrinfo led to memory corruption and a potentially exploitable crash. *Note: This issue only affected Linux operating systems. Other operating systems are unaffected.* This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29986**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://www.mozilla.org/security/advisories/mfsa2021-35/	A-MOZ-FIRE-020921/272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Interpretation Conflict	17-Aug-21	6.8	Firefox incorrectly treated an inline list-item element as a block element, resulting in an out of bounds read or memory corruption, and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29988**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://www.mozilla.org/security/advisories/mfsa2021-35/	A-MOZ-FIRE-020921/273
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 90 and Firefox ESR 78.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.13, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29989**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-35/	A-MOZ-FIRE-020921/274
thunderbird					
Missing Initialization of Resource	17-Aug-21	6.8	Uninitialized memory in a canvas object could have caused an incorrect free() leading to memory corruption	https://bugzilla.mozilla.org/show_bug.cgi?id=17222	A-MOZ-THUN-020921/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29980**	04, https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/	
N/A	17-Aug-21	6.8	An issue present in lowering/register allocation could have led to obscure but deterministic register confusion failures in JITted code that would lead to a potentially exploitable crash. This vulnerability affects Firefox < 91 and Thunderbird < 91. **CVE ID : CVE-2021-29981**	https://bugzilla.mozilla.org/show_bug.cgi?id=1707774, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/	A-MOZ-THUN-020921/276
Missing Release of Resource after Effective Lifetime	17-Aug-21	4.3	Due to incorrect JIT optimization, we incorrectly interpreted data from the wrong type of object, resulting in the potential leak of a single bit of memory. This vulnerability affects Firefox < 91 and Thunderbird < 91. **CVE ID : CVE-2021-29982**	https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2	A-MOZ-THUN-020921/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				021-36/, https://bugzilla.mozilla.org/show_bug.cgi?id=1715318	
N/A	17-Aug-21	6.8	Instruction reordering resulted in a sequence of instructions that would cause an object to be incorrectly considered during garbage collection. This led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29984**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://www.mozilla.org/security/advisories/mfsa2021-35/	A-MOZ-THUN-020921/278
Use After Free	17-Aug-21	6.8	A use-after-free vulnerability in media channels could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29985**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2	A-MOZ-THUN-020921/279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				021-36/, https://www.mozilla.org/security/advisories/mfsa2021-35/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Aug-21	6.8	A suspected race condition when calling getaddrinfo led to memory corruption and a potentially exploitable crash. *Note: This issue only affected Linux operating systems. Other operating systems are unaffected.* This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29986**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://www.mozilla.org/security/advisories/mfsa2021-35/	A-MOZ-THUN-020921/280
Improper Restriction of Excessive Authentication Attempts	17-Aug-21	4.3	After requesting multiple permissions, and closing the first permission panel, subsequent permission panels will be displayed in a different position but still record a click in the default location, making it possible to trick a user into accepting a permission they did not want to. *This bug only affects Firefox on Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox < 91 and	https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://bugzilla.mozilla.org/show_bug.cgi?id=17161	A-MOZ-THUN-020921/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 91. **CVE ID : CVE-2021-29987**	29	
Interpretation Conflict	17-Aug-21	6.8	Firefox incorrectly treated an inline list-item element as a block element, resulting in an out of bounds read or memory corruption, and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29988**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://www.mozilla.org/security/advisories/mfsa2021-35/	A-MOZ-THUN-020921/282
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 90 and Firefox ESR 78.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.13, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29989**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-35/	A-MOZ-THUN-020921/283
multiplayer-plugin_project					
multiplayer-plugin					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The Multiplayer Games WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of $_SERVER['PHP_SELF'] in the ~/multiplayergames.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.7. **CVE ID : CVE-2021-34644**	N/A	A-MUL-MULT-020921/284
Nextcloud					
desktop					
Untrusted Search Path	18-Aug-21	4.4	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server with a computer. The Nextcloud Desktop Client invokes its uninstaller script when being installed to make sure there are no remnants of previous installations. In versions 3.0.3 through 3.2.4, the Client searches the `Uninstall.exe` file in a folder that can be written by regular users. This could lead to a case where a malicious user creates a malicious `Uninstall.exe`, which would be executed with administrative privileges on the Nextcloud Desktop Client installation. This issue is fixed in Nextcloud Desktop Client version 3.3.0. As a workaround, do not allow untrusted users to create content in the `C:\` system folder and verify that there is no malicious `C:\Uninstall.exe`	https://github.com/nextcloud/desktop/pull/3497, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-6q2w-v879-q24v	A-NEX-DESK-020921/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file on the system. **CVE ID : CVE-2021-37617**		
nextcloud					
Improper Certificate Validation	18-Aug-21	4	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server with a computer. Clients using the Nextcloud end-to-end encryption feature download the public and private key via an API endpoint. In versions prior to 3.3.0, the Nextcloud Desktop client fails to check if a private key belongs to previously downloaded public certificate. If the Nextcloud instance serves a malicious public key, the data would be encrypted for this key and thus could be accessible to a malicious actor. This issue is fixed in Nextcloud Desktop Client version 3.3.0. There are no known workarounds aside from upgrading. **CVE ID : CVE-2021-32728**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-f5fr-5gcv-6cc5, https://github.com/nextcloud/desktop/pull/3338	A-NEX-NEXT-020921/286
nic					
knot_resolver					
Reachable Assertion	25-Aug-21	5	Knot Resolver before 5.3.2 is prone to an assertion failure, triggerable by a remote attacker in an edge case (NSEC3 with too many iterations used for a positive wildcard proof). **CVE ID : CVE-2021-40083**	https://gitlab.nic.cz/knot/knot-resolver/-/merge_requests/1169	A-NIC-KNOT-020921/287
nimble3					
m-vslider					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-21	6.5	The update functionality in the rslider_page uses an rs_id POST parameter which is not validated, sanitised or escaped before being inserted in sql query, therefore leading to SQL injection for users having Administrator role. **CVE ID : CVE-2021-24557**	N/A	A-NIM-M-VS-020921/288
Nodejs					
node.js					
Improper Input Validation	16-Aug-21	7.5	Node.js before 16.6.0, 14.17.4, and 12.22.4 is vulnerable to Remote Code Execution, XSS, Application crashes due to missing input validation of host names returned by Domain Name Servers in Node.js dns library which can lead to output of wrong hostnames (leading to Domain Hijacking) and injection vulnerabilities in applications using the library. **CVE ID : CVE-2021-22931**	https://nodejs.org/en/blog/vulnerability/aug-2021-security-releases/	A-NOD-NODE-020921/289
Improper Certificate Validation	16-Aug-21	5	If the Node.js https API was used incorrectly and "undefined" was in passed for the "rejectUnauthorized" parameter, no error was returned and connections to servers with an expired certificate would have been accepted. **CVE ID : CVE-2021-22939**	https://nodejs.org/en/blog/vulnerability/aug-2021-security-releases/	A-NOD-NODE-020921/290
Use After Free	16-Aug-21	5	Node.js before 16.6.1, 14.17.5, and 12.22.5 is vulnerable to a use after free attack where an	https://nodejs.org/en/blog/vulnerabili	A-NOD-NODE-020921/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker might be able to exploit the memory corruption, to change process behavior. **CVE ID : CVE-2021-22940**	ty/aug-2021-security-releases/	
octopus					
octopus_server					
Cleartext Storage of Sensitive Information	18-Aug-21	5	In Octopus Server after version 2018.8.2 if the Octopus Server Web Request Proxy is configured with authentication, the password is shown in plaintext in the UI. **CVE ID : CVE-2021-31820**	https://advisories.octopus.com/adv/2021-07---Proxy-Password-Stored-in-Plaintext-(CVE-2021-31820).2193063986.html	A-OCT-OCTO-020921/292
oculus					
desktop					
Improper Privilege Management	19-Aug-21	4.6	Due to a bug with management of handles in OVRServiceLauncher.exe, an attacker could expose a privileged process handle to an unprivileged process, leading to local privilege escalation. This issue affects Oculus Desktop versions after 1.39 and prior to 31.1.0.67.507. **CVE ID : CVE-2021-24038**	https://www.facebook.com/security/advisories/cve-2021-24038	A-OCU-DESK-020921/293
onenav					
onenav					
Exposure of Resource to Wrong Sphere	16-Aug-21	5	OneNav 0.9.12 allows Information Disclosure of the onenav.db3 contents. NOTE: the vendor's recommended	N/A	A-ONE-ONEN-020921/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			solution is to block the access via an NGINX configuration file. **CVE ID : CVE-2021-38712**		
online_catering_reservation_system_project					
online_catering_reservation_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	A cross-site scripting (XSS) vulnerability in Online Catering Reservation System using PHP on Sourcecodester allows an attacker to arbitrarily inject code in the search bar. **CVE ID : CVE-2021-38752**	N/A	A-ONL-ONLI-020921/295
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Aug-21	5	Directory traversal vulnerability in Online Catering Reservation System 1.0 exists due to lack of validation in index.php. **CVE ID : CVE-2021-38758**	N/A	A-ONL-ONLI-020921/296
Openstack					
neutron					
Incorrect Authorization	23-Aug-21	5.8	OpenStack Neutron before 16.4.1, 17.x before 17.1.3, and 18.0.0 allows hardware address impersonation when the linuxbridge driver with ebtables-nft is used on a Netfilter-based platform. By sending carefully crafted packets, anyone in control of a server instance connected to the virtual switch can impersonate the hardware addresses of other systems on the network, resulting in	N/A	A-OPE-NEUT-020921/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service or in some cases possibly interception of traffic intended for other destinations. **CVE ID : CVE-2021-38598**		
osgeo					
pywps					
Improper Restriction of XML External Entity Reference	23-Aug-21	5	An XML external entity (XXE) injection in PyWPS before 4.5.0 allows an attacker to view files on the application server filesystem by assigning a path to the entity. OWSLib 0.24.1 may also be affected. **CVE ID : CVE-2021-39371**	https://github.com/geopython/pywps/pull/616, https://github.com/geopython/OWSLib/issues/790	A-OSG-PYWP-020921/298
Owasp					
csrfguard					
Cross-Site Request Forgery (CSRF)	19-Aug-21	6.8	In OWASP CSRFGuard through 3.1.0, CSRF can occur because the CSRF cookie may be retrieved by using only a session token. **CVE ID : CVE-2021-28490**	N/A	A-OWA-CSRF-020921/299
pac-resolver_project					
pac-resolver					
N/A	24-Aug-21	7.5	This affects the package pac-resolver before 5.0.0. This can occur when used with untrusted input, due to unsafe PAC file handling. **NOTE:** The fix for this vulnerability is applied in the node-degenerator library, a dependency written by the same maintainer. **CVE ID : CVE-2021-23406**	https://github.com/TooTallNate/node-degenerator/commit/9d25bb67d957bc2e5425fea7bf7a58b3fc64ff9e, https://github.com/TooTallNate/node-	A-PAC-PAC--020921/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				degenerator/commit/ccc34453541353 98b6eb1a04c7d27c13b833f2d5, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1568506	
phonetrack					
phonetrack_meu_site_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	The PhoneTrack Meu Site Manager WordPress plugin through 0.1 does not sanitise or escape its "php_id" setting before outputting it back in an attribute in the page, leading to a stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24534**	N/A	A-PHO-PHON-020921/301
Pimcore					
pimcore					
Improper Neutralization of Formula Elements in a CSV File	18-Aug-21	6.5	Pimcore is an open source data & experience management platform. Prior to version 10.1.1, Data Object CSV import allows formular injection. The problem is patched in 10.1.1. Aside from upgrading, one may apply the patch manually as a workaround. **CVE ID : CVE-2021-37702**	https://github.com/pimcore/pimcore/security/advisories/GHSA-pp2h-95hm-hv9r, https://github.com/pimcore/pimcore/pull/9992	A-PIM-PIMC-020921/302
Pingidentity					
rsa_securid_integration_kit					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Origin Validation Error	18-Aug-21	5	In Ping Identity RSA SecurID Integration Kit before 3.2, user impersonation can occur. **CVE ID : CVE-2021-39270**	https://docs.pingidentity.com/bundle/integrations/page/yqq1563995045546.html	A-PIN-RSA_-020921/303
Pixelimity					
Pixelimity					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-21	3.5	Cross Site Scripting (XSS) vulnerability exists in Pixelimity 1.0 via the HTTP POST parameter to admin/setting.php. **CVE ID : CVE-2021-29056**	N/A	A-PIX-PIXE-020921/304
plib_project					
plib					
Integer Overflow or Wraparound	24-Aug-21	9.3	In Plib through 1.85, there is an integer overflow vulnerability that could result in arbitrary code execution. The vulnerability is found in ssgLoadTGA() function in src/ssg/ssgLoadTGA.cxx file. **CVE ID : CVE-2021-38714**	N/A	A-PLI-PLIB-020921/305
popojicms					
popojicms					
Cross-Site Request Forgery (CSRF)	25-Aug-21	4.3	Cross Site Request Forgery (CSRF) vulnerability exist in PopojiCMS 2.0.1 in po-admin/route.php?mod=user&act=multidelete. **CVE ID : CVE-2021-28070**	N/A	A-POP-POPO-020921/306
prestahome					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
blog					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-21	5	A SQL Injection issue in the list controller of the Prestahome Blog (aka ph_simpleblog) module before 1.7.8 for Prestashop allows a remote attacker to extract data from the database via the sb_category parameter. **CVE ID : CVE-2021-36748**	N/A	A-PRE-BLOG-020921/307
proxyee-down_project					
proxyee-down					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Aug-21	9.3	Proxyee-Down is open source proxy software. An attacker being able to provide an extension script (eg: through a MiTM attack or by hosting a malicious extension) may be able to run arbitrary commands on the system running Proxyee-Down. For more details including a PoC see the referenced GHSL-2021-053. As of the writing of this CVE there is currently no patched version. **CVE ID : CVE-2021-32826**	https://securitylab.github.com/advisories/GHSL-2021-053-proxyee-down/	A-PRO-PROX-020921/308
Pulsesecure					
pulse_connect_secure					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Aug-21	5.5	A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform an arbitrary file delete via a maliciously crafted web request. **CVE ID : CVE-2021-22933**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44858/?kA23Z000000L6oySAC	A-PUL-PULS-020921/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Aug-21	6.5	A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator or compromised Pulse Connect Secure device in a load-balanced configuration to perform a buffer overflow via a malicious crafted web request. **CVE ID : CVE-2021-22934**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44858/?kA23Z000000L6oySAC	A-PUL-PULS-020921/310
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Aug-21	6.5	A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform command injection via an unsanitized web parameter. **CVE ID : CVE-2021-22935**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44858/?kA23Z000000L6oySAC	A-PUL-PULS-020921/311
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	A vulnerability in Pulse Connect Secure before 9.1R12 could allow a threat actor to perform a cross-site script attack against an authenticated administrator via an unsanitized web parameter. **CVE ID : CVE-2021-22936**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44858/?kA23Z000000L6oySAC	A-PUL-PULS-020921/312
Unrestricted Upload of File with Dangerous Type	16-Aug-21	6.5	A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform a file write via a maliciously crafted archive uploaded in the administrator web interface. **CVE ID : CVE-2021-22937**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44858/?kA23Z000000L6oySAC	A-PUL-PULS-020921/313
Improper Neutralization of Special Elements used in a	16-Aug-21	6.5	A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform command injection via an	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA	A-PUL-PULS-020921/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			unsanitized web parameter in the administrator web console. **CVE ID : CVE-2021-22938**	44858/?kA23Z000000L6oySAC	
quantumcloud					
slider_hero					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-21	6.5	The Slider Hero with Animation, Video Background & Intro Maker WordPress plugin before 8.2.7 does not sanitise or escape the id attribute of its hero-button shortcode before using it in a SQL statement, allowing users with a role as low as Contributor to perform SQL injection. **CVE ID : CVE-2021-24506**	N/A	A-QUA-SLID-020921/315
Rapid7					
nexpose					
Missing Authentication for Critical Function	19-Aug-21	5.5	Rapid7 Nexpose version 6.6.95 and earlier allows authenticated users of the Security Console to view and edit any ticket in the legacy ticketing feature, regardless of the assignment of the ticket. This issue was resolved in version 6.6.96, released on August 4, 2021. **CVE ID : CVE-2021-31868**	https://docs.rapid7.com/release-notes/nexpose/20210804/	A-RAP-NEXP-020921/316
Realtek					
jungle_sdk					
Out-of-bounds Write	16-Aug-21	7.8	Realtek Jungle SDK version v2.x up to v3.4.14B provides a 'WiFi Simple Config' server that implements both UPnP and SSDP protocols. The	https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en,	A-REA-JUNG-020921/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			binary is usually named wscd or mini_upnpd and is the successor to miniigd. The server is vulnerable to a heap buffer overflow that is present due to unsafe crafting of SSDP NOTIFY messages from received M-SEARCH messages ST header. **CVE ID : CVE-2021-35392**	https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf	
realtek_jungle_sdk					
Out-of-bounds Write	16-Aug-21	10	Realtek Jungle SDK version v2.x up to v3.4.14B provides a 'WiFi Simple Config' server that implements both UPnP and SSDP protocols. The binary is usually named wscd or mini_upnpd and is the successor to miniigd. The server is vulnerable to a stack buffer overflow vulnerability that is present due to unsafe parsing of the UPnP SUBSCRIBE/UNSUBSCRIBE Callback header. Successful exploitation of this vulnerability allows remote unauthenticated attackers to gain arbitrary code execution on the affected device. **CVE ID : CVE-2021-35393**	https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en, https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf	A-REA-REAL-020921/318
N/A	16-Aug-21	10	Realtek Jungle SDK version v2.x up to v3.4.14B provides a diagnostic tool called 'MP Daemon' that is usually compiled as 'UDPServer' binary. The binary is affected by multiple memory corruption vulnerabilities and	https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en, https://www.realtek.com/images/safe-	A-REA-REAL-020921/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an arbitrary command injection vulnerability that can be exploited by remote unauthenticated attackers. **CVE ID : CVE-2021-35394**	report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Aug-21	10	Realtek Jungle SDK version v2.x up to v3.4.14B provides an HTTP web server exposing a management interface that can be used to configure the access point. Two versions of this management interface exists: one based on Go-Ahead named webs and another based on Boa named boa. Both of them are affected by these vulnerabilities. Specifically, these binaries are vulnerable to the following issues: - stack buffer overflow in formRebootCheck due to unsafe copy of submit-url parameter - stack buffer overflow in formWsc due to unsafe copy of submit-url parameter - stack buffer overflow in formWlanMultipleAP due to unsafe copy of submit-url parameter - stack buffer overflow in formWlSiteSurvey due to unsafe copy of ifname parameter - stack buffer overflow in formStaticDHCP due to unsafe copy of hostname parameter - stack buffer overflow in formWsc due to unsafe copy of 'peerPin' parameter - arbitrary	https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en, https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf	A-REA-REAL-020921/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command execution in formSysCmd via the sysCmd parameter - arbitrary command injection in formWsc via the 'peerPin' parameter Exploitability of identified issues will differ based on what the end vendor/manufacturer did with the Realtek SDK webserver. Some vendors use it as-is, others add their own authentication implementation, some kept all the features from the server, some remove some of them, some inserted their own set of features. However, given that Realtek SDK implementation is full of insecure calls and that developers tends to re-use those examples in their custom code, any binary based on Realtek SDK webserver will probably contains its own set of issues on top of the Realtek ones (if kept). Successful exploitation of these issues allows remote attackers to gain arbitrary code execution on the device. **CVE ID : CVE-2021-35395**		
recaptcha_solver_project					
recaptcha_solver					
Improper Neutralization of Input During Web Page Generation	22-Aug-21	4.3	An XSS issue was discovered in ReCaptcha Solver 5.7. A response from Anti-Captcha.com, RuCaptcha.com, 2captcha.com, DEATHbyCAPTCHA.com,	N/A	A-REC-RECA-020921/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			ImageTyperz.com, or BestCaptchaSolver.com in setCaptchaCode() is inserted into the DOM as HTML, resulting in full control over the user's browser by these servers. **CVE ID : CVE-2021-39362**		
roosty					
diary-availability-calendar					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-21	6.5	The daac_delete_booking_callback function, hooked to the daac_delete_booking AJAX action, takes the id POST parameter which is passed into the SQL statement without proper sanitisation, validation or escaping, leading to a SQL Injection issue. Furthermore, the ajax action is lacking any CSRF and capability check, making it available to any authenticated user. **CVE ID : CVE-2021-24555**	N/A	A-ROO-DIAR-020921/322
salesagility					
suitecrm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Aug-21	4.3	Persistent cross-site scripting (XSS) in the web interface of SuiteCRM before 7.11.19 allows a remote attacker to introduce arbitrary JavaScript via a Content-Type Filter bypass to upload malicious files. This occurs because text/html is blocked, but other types that allow JavaScript execution (such as text/xml)	https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_19	A-SAL-SUIT-020921/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are not blocked. **CVE ID : CVE-2021-39267**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Aug-21	4.3	Persistent cross-site scripting (XSS) in the web interface of SuiteCRM before 7.11.19 allows a remote attacker to introduce arbitrary JavaScript via malicious SVG files. This occurs because the clean_file_output protection mechanism can be bypassed. **CVE ID : CVE-2021-39268**	https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_19	A-SAL-SUIT-020921/324
satollo					
giveaway					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-21	6.5	The Giveaway WordPress plugin through 1.2.2 is vulnerable to an SQL Injection issue which allows an administrative user to execute arbitrary SQL commands via the $post_id on the options.php page. **CVE ID : CVE-2021-24497**	N/A	A-SAT-GIVE-020921/325
scribblemaps					
scribble_maps					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The Scribble Maps WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the map parameter in the ~/includes/admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2. **CVE ID : CVE-2021-34651**	N/A	A-SCR-SCRI-020921/326
seacms					
seacms					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-21	4.3	Cross Site Scripting (XSS) vulnerability exists in SeaCMS 12.6 via the (1) v_company and (2) v_tvs parameters in /admin_video.php, **CVE ID : CVE-2021-29313**	N/A	A-SEA-SEAC-020921/327
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Aug-21	7.5	SQL Injection in SEACMS v210530 (2021-05-30) allows remote attackers to execute arbitrary code via the component "admin_ajax.php?action=checkrepeat&v_name=". **CVE ID : CVE-2021-37358**	N/A	A-SEA-SEAC-020921/328
seopress					
seopress					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	The SEOPress WordPress plugin is vulnerable to Stored Cross-Site-Scripting via the processPut function found in the ~/src/Actions/Api/TitleDescriptionMeta.php file which allows authenticated attackers to inject arbitrary web scripts, in versions 5.0.0 - 5.0.3. **CVE ID : CVE-2021-34641**	N/A	A-SEO-SEOP-020921/329
shantz_wordpress_qotd_project					
shantz_wordpress_qotd					
Cross-Site Request Forgery (CSRF)	16-Aug-21	4.3	The Shantz WordPress QOTD WordPress plugin through 1.2.2 is lacking any CSRF check when updating its settings, allowing attackers to make logged in administrators	N/A	A-SHA-SHAN-020921/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			change them to arbitrary values. **CVE ID : CVE-2021-24380**		
Shopware					
shopware					
N/A	16-Aug-21	5	Shopware is an open source eCommerce platform. Versions prior to 6.4.3.1 contain a vulnerability that allows manipulation of product reviews via API. Version 6.4.3.1 contains a patch. As workarounds for older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin. **CVE ID : CVE-2021-37707**	https://github.com/shopware/platform/security/advisories/GHSA-9f8f-574q-8jmf, https://github.com/shopware/platform/commit/912b96de3b839c6c5525c98cbb58f537c2d838be	A-SHO-SHOP-020921/331
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Aug-21	7.5	Shopware is an open source eCommerce platform. Versions prior to 6.4.3.1 contain a command injection vulnerability in mail agent settings. Version 6.4.3.1 contains a patch. As workarounds for older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin. **CVE ID : CVE-2021-37708**	https://github.com/shopware/platform/commit/82d8d1995f6ce9054323b2c3522b1b3cf04853aa, https://github.com/shopware/platform/security/advisories/GHSA-xh55-2fqp-p775	A-SHO-SHOP-020921/332
Insertion of Sensitive Information into Log File	16-Aug-21	4	Shopware is an open source eCommerce platform. Versions prior to 6.4.3.1 contain a vulnerability involving an	https://github.com/shopware/platform/security/a	A-SHO-SHOP-020921/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insecure direct object reference of log files of the Import/Export feature. Version 6.4.3.1 contains a patch. As workarounds for older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin. **CVE ID : CVE-2021-37709**	dvisories/GHSA-54gp-qff8-946c, https://github.com/shopware/platform/commit/a9f52abb6eb503654c492b6b2076f8d924831fec	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	Shopware is an open source eCommerce platform. Versions prior to 6.4.3.1 contain a Cross-Site Scripting vulnerability via SVG media files. Version 6.4.3.1 contains a patch. As workarounds for older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin. **CVE ID : CVE-2021-37710**	https://github.com/shopware/platform/security/advisories/GHSA-fc38-mxwr-pfhx, https://github.com/shopware/platform/commit/abe9f69e1f667800f974accd3047b4930e4b423	A-SHO-SHOP-020921/334
Server-Side Request Forgery (SSRF)	16-Aug-21	6.5	Versions prior to 6.4.3.1 contain an authenticated server-side request forgery vulnerability in file upload via URL. Version 6.4.3.1 contains a patch. As workarounds for older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin. **CVE ID : CVE-2021-37711**	https://github.com/shopware/platform/security/advisories/GHSA-gcvv-gq92-x94r, https://github.com/shopware/platform/commit/b9f330e652b743dd2374c02bbe68f28b5	A-SHO-SHOP-020921/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				9a3f502	
Siemens					
sinema_remote_connect					
N/A	19-Aug-21	4.6	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.0 SP1). Affected devices allow to modify configuration settings over an unauthenticated channel. This could allow a local attacker to escalate privileges and execute own code on the device. **CVE ID : CVE-2021-31338**	https://cert-portal.siemens.com/productcert/pdf/ssa-816035.pdf	A-SIE-SINE-020921/336
simple-behace-portfolio_project					
simple-behace-portfolio					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The Simple Behance Portfolio WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `dark` parameter in the ~/titan-framework/iframe-font-preview.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.2. **CVE ID : CVE-2021-34649**	N/A	A-SIM-SIMP-020921/337
simple_banner_project					
simple_banner					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	3.5	The Simple Banner WordPress plugin before 2.10.4 does not sanitise and escape one of its settings, allowing high privilege users such as admin to use Cross-Site Scripting payload even when the unfiltered_html capability is	https://plugins.trac.wordpress.org/changeset/2571047/	A-SIM-SIMP-020921/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disallowed. **CVE ID : CVE-2021-24574**		
simple_events_calendar_project					
simple_events_calendar					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-21	6.5	The Simple Events Calendar WordPress plugin through 1.4.0 does not sanitise, validate or escape the event_id POST parameter before using it in a SQL statement when deleting events, leading to an authenticated SQL injection issue **CVE ID : CVE-2021-24552**	N/A	A-SIM-SIMP-020921/339
simple_image_gallery_web_app_project					
simple_image_gallery_web_app					
Unrestricted Upload of File with Dangerous Type	16-Aug-21	7.5	An unrestricted file upload on Simple Image Gallery Web App can be exploited to upload a web shell and executed to gain unauthorized access to the server hosting the web app. **CVE ID : CVE-2021-38753**	N/A	A-SIM-SIMP-020921/340
sizmic					
plugmatter_pricing_table					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The Plugmatter Pricing Table Lite WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `email` parameter in the ~/license.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.32. **CVE ID : CVE-2021-34659**	N/A	A-SIZ-PLUG-020921/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
skaut-bazar_project					
skaut-bazar					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The Skaut bazar WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of $_SERVER['PHP_SELF'] in the ~/skaut-bazar.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.3.2. **CVE ID : CVE-2021-34643**	N/A	A-SKA-SKAU-020921/342
Smartypantsplugins					
sp_project_\\&_document_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The SP Project & Document Manager WordPress plugin is vulnerable to attribute-based Reflected Cross-Site Scripting via the from and to parameters in the ~/functions.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 4.25. **CVE ID : CVE-2021-38315**	N/A	A-SMA-SP_P-020921/343
social_tape_project					
social_tape					
Cross-Site Request Forgery (CSRF)	16-Aug-21	4.3	The Social Tape WordPress plugin through 1.0 does not have CSRF checks in place when saving its settings, and do not sanitise or escape them before outputting them back in the page, leading to a stored Cross-Site Scripting issue via a CSRF attack	N/A	A-SOC-SOCI-020921/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24411		
Sqlite					
sqlite					
Out-of-bounds Read	24-Aug-21	5	** DISPUTED ** A segmentation fault can occur in the sqlite3.exe command-line component of SQLite 3.36.0 via the idxGetTableInfo function when there is a crafted SQL query. NOTE: the vendor disputes the relevance of this report because a sqlite3.exe user already has full privileges (e.g., is intentionally allowed to execute commands). This report does NOT imply any problem in the SQLite library. **CVE ID : CVE-2021-36690**	https://www.sqlite.org/forum/forumpost/718c0a8d17	A-SQL-SQLI-020921/345
startserver_project					
startserver					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Aug-21	5	All versions of package startserver are vulnerable to Directory Traversal due to missing sanitization. **CVE ID : CVE-2021-23430**	N/A	A-STA-STAR-020921/346
telugu_bible_verse_daily_project					
telugu_bible_verse_daily					
Cross-Site Request Forgery (CSRF)	16-Aug-21	4.3	The à°¤à±†à°²à±?à°—à±? à°¬à±ˆà°¬à°¿à°²à±? à°µà°šà°¨à°®à±?à°²à±? WordPress plugin through 1.0 is lacking any CSRF check when saving its settings and verses, and do not sanitise or	N/A	A-TEL-TELU-020921/347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escape them when outputting them back in the page. This could allow attackers to make a logged in admin change the settings, as well as add malicious verses containing JavaScript code in them, leading to Stored XSS issues **CVE ID : CVE-2021-24410**		
Textpattern					
textpattern					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Aug-21	3.5	A cross-site scripting vulnerability was discovered in the Comments parameter in Textpattern CMS 4.8.4 which allows remote attackers to execute arbitrary code via a crafted payload entered into the URL field. The vulnerability is triggered by users visiting https://site.com/articles/welcome-to-your-site#comments-head. **CVE ID : CVE-2021-28001**	N/A	A-TEX-TEXT-020921/348
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Aug-21	3.5	A persistent cross-site scripting vulnerability was discovered in the Excerpt parameter in Textpattern CMS 4.9.0 which allows remote attackers to execute arbitrary code via a crafted payload entered into the URL field. The vulnerability is triggered by users visiting the 'Articles' page. **CVE ID : CVE-2021-28002**	N/A	A-TEX-TEXT-020921/349
throughtek					
kalay_p2p_software_development_kit					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	17-Aug-21	7.6	ThroughTek's Kalay Platform 2.0 network allows an attacker to impersonate an arbitrary ThroughTek (TUTK) device given a valid 20-byte uniquely assigned identifier (UID). This could result in an attacker hijacking a victim's connection and forcing them into supplying credentials needed to access the victim TUTK device. **CVE ID : CVE-2021-28372**	https://www.throughtek.com/kalay_overview.html	A-THR-KALA-020921/350
timeline_calendar_project					
timeline_calendar					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-21	6.5	The Timeline Calendar WordPress plugin through 1.2 does not sanitise, validate or escape the edit GET parameter before using it in a SQL statement when editing events, leading to an authenticated SQL injection issue. Other SQL Injections are also present in the plugin **CVE ID : CVE-2021-24553**	N/A	A-TIM-TIME-020921/351
tranquil					
wapt					
Incorrect Authorization	16-Aug-21	7.2	Incorrect Access Control in Tranquil WAPT Enterprise - before 1.8.2.7373 and before 2.0.0.9450 allows guest OS users to escalate privileges via WAPT Agent. **CVE ID : CVE-2021-38608**	https://www.wapt.fr/fr/doc/wapt-security-bulletin.html, https://www.tranquil.it/en/manage-it-equipment/discover-	A-TRA-WAPT-020921/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				wapt/	
transpile_project					
transpile					
Improper Handling of Exceptional Conditions	24-Aug-21	5	All versions of package transpile are vulnerable to Denial of Service (DoS) due to a lack of input sanitization or whitelisting, coupled with improper exception handling in the .to() function. **CVE ID : CVE-2021-23429**	N/A	A-TRA-TRAN-020921/353
trim-off-newlines_project					
trim-off-newlines					
N/A	18-Aug-21	5	All versions of package trim-off-newlines are vulnerable to Regular Expression Denial of Service (ReDoS) via string processing. **CVE ID : CVE-2021-23425**	N/A	A-TRI-TRIM-020921/354
typofr_project					
typofr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The 2TypoFR WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the text function found in the ~/vendor/Org_Heigl/Hyphenator/index.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.11. **CVE ID : CVE-2021-34657**	N/A	A-TYP-TYPO-020921/355
vehicle_parking_management_system_project					
vehicle_parking_management_system					
Improper	19-Aug-21	3.5	A persistent cross site	N/A	A-VEH-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			scripting (XSS) vulnerability in the Add Categories module of Vehicle Parking Management System 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the Category field. **CVE ID : CVE-2021-27822**		VEHI-020921/356
veronalabs					
wp_sms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	3.5	The WP SMS WordPress plugin before 5.4.13 does not sanitise the "wp_group_name" parameter before outputting it back in the "Groups" page, leading to an Authenticated Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24561**	https://plugins.trac.wordpress.org/changeset/2570762/wp-sms	A-VER-WP_S-020921/357
verse-o-matic_project					
verse-o-matic					
Cross-Site Request Forgery (CSRF)	16-Aug-21	4.3	The Verse-O-Matic WordPress plugin through 4.1.1 does not have any CSRF checks in place, allowing attackers to make logged in administrators do unwanted actions, such as add/edit/delete arbitrary verses and change the settings. Due to the lack of sanitisation in the settings and verses, this could also lead to Stored Cross-Site Scripting issues **CVE ID : CVE-2021-24466**	N/A	A-VER-VERS-020921/358
Videowhisper					
2way_videocalls_and_random_chat					
Improper	16-Aug-21	4.3	The 2Way VideoCalls and	N/A	A-VID-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			Random Chat - HTML5 Webcam Videochat WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `vws_notice` function found in the ~/inc/requirements.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 5.2.7. **CVE ID : CVE-2021-34656**		2WAY-020921/359
video_posts_webcam_recorder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	The Video Posts Webcam Recorder WordPress plugin before 3.2.4 has an authenticated reflected cross site scripting (XSS) vulnerability in one of the administrative functions for handling deletion of videos. **CVE ID : CVE-2021-24512**	N/A	A-VID-VIDE-020921/360
vikwp					
car_rental_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	The VikRentCar Car Rental Management System WordPress plugin before 1.1.10 does not sanitise the 'Text Next to Icon' field when adding or editing a Characteristic, allowing high privilege users such as admin to use XSS payload in it, leading to an authenticated Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24519**	N/A	A-VIK-CAR_-020921/361
webfactoryltd					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
maintenance					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	3.5	The Maintenance WordPress plugin before 4.03 does not sanitise or escape some of its settings, allowing high privilege users such as admin to se Cross-Site Scripting payload in them (even when the unfiltered_html capability is disallowed), which will be triggered in the frontend **CVE ID : CVE-2021-24533**	N/A	A-WEB-MAIN-020921/362
webrecorder					
pywb					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Aug-21	4.3	Webrecorder pywb before 2.6.0 allows XSS because it does not ensure that Jinja2 templates are autoescaped. **CVE ID : CVE-2021-39286**	https://github.com/webrecorder/pywb/commit/f7bd84cdacdd665ff73ae8d09a202f60be2ebae9	A-WEB-PYWB-020921/363
Wonderplugin					
wonder_pdf_embed					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	The Wonder PDF Embed WordPress plugin before 1.7 does not escape parameters of its wonderplugin_pdf shortcode, which could allow users with a role as low as Contributor to perform Stored XSS attacks. **CVE ID : CVE-2021-24541**	N/A	A-WON-WOND-020921/364
wonder_video_embed					
Improper Neutralization of Input	16-Aug-21	3.5	The Wonder Video Embed WordPress plugin before 1.8 does not escape parameters of	N/A	A-WON-WOND-020921/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			its wonderplugin_video shortcode, which could allow users with a role as low as Contributor to perform Stored XSS attacks. **CVE ID : CVE-2021-24540**		
wpbrigade					
simple_social_media_share_buttons					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	3.5	The Simple Social Media Share Buttons â€“ Social Sharing for Everyone WordPress plugin before 3.2.3 did not escape the align and like_button_size parameters of its SSB shortcode, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2021-24486**	N/A	A-WPB-SIMP-020921/366
wpcerber					
wp_cerber					
Improper Authentication	19-Aug-21	7.5	WP Cerber before 8.9.3 allows MFA bypass via wordpress_logged_in_[hash] manipulation. **CVE ID : CVE-2021-37597**	N/A	A-WPC-WP_C-020921/367
Incorrect Authorization	19-Aug-21	5	WP Cerber before 8.9.3 allows bypass of /wp-json access control via a trailing ? character. **CVE ID : CVE-2021-37598**	N/A	A-WPC-WP_C-020921/368
wpcharitable					
charitable					
Improper Neutralization of Input	23-Aug-21	3.5	The Charitable â€“ Donation Plugin WordPress plugin before 1.6.51 is affected by an	https://www.wpcharitable.com/release	A-WPC-CHAR-020921/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			authenticated stored cross-site scripting vulnerability which was found in the add donation feature. **CVE ID : CVE-2021-24531**	-notes-1-6-51/	
Wpeasycart					
shopping_cart_\\&_ecommerce_store					
Cross-Site Request Forgery (CSRF)	19-Aug-21	6.8	The Shopping Cart & eCommerce Store WordPress plugin is vulnerable to Cross-Site Request Forgery via the save_currency_settings function found in the ~/admin/inc/wp_easycart_admin_initial_setup.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 5.1.0. **CVE ID : CVE-2021-34645**	https://plugins.trac.wordpress.org/browser/wp-easycart/trunk/admin/inc/wp_easycart_admin_initial_setup.php?rev=2463792#L240	A-WPE-SHOP-020921/370
wpfront					
notification_bar					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	3.5	The WPFront Notification Bar WordPress plugin before 2.0.0.07176 does not sanitise or escape its Custom CSS setting, allowing high privilege users such as admin to set XSS payload in it even when the unfiltered_html capability is disallowed, leading to an authenticated Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24518**	N/A	A-WPF-NOTI-020921/371
scroll_top					
Improper Neutralizatio	23-Aug-21	3.5	The WPFront Scroll Top WordPress plugin before	N/A	A-WPF-SCRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			2.0.6.07225 does not sanitise or escape its Image ALT setting before outputting it attributes, leading to an Authenticated Stored Cross-Site Scripting issues even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24564**		020921/372
wp_fountain_project					
wp_fountain					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The WP Fountain WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of $_SERVER['PHP_SELF'] in the ~/wp-fountain.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.5.9. **CVE ID : CVE-2021-34653**	N/A	A-WP_-WP_F-020921/373
wp_seo_tags_project					
wp_seo_tags					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	4.3	The WP SEO Tags WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the saq_txt_the_filter parameter in the ~/wp-seo-tags.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.2.7. **CVE ID : CVE-2021-34665**	N/A	A-WP_-WP_S-020921/374
wp_songbook_project					
wp_songbook					
Improper	16-Aug-21	4.3	The WP Songbook WordPress	N/A	A-WP_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			plugin is vulnerable to Reflected Cross-Site Scripting via the url parameter found in the ~/inc/class.ajax.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.11. **CVE ID : CVE-2021-34655**		WP_S-020921/375
xerosecurity					
sn1per					
Incorrect Default Permissions	19-Aug-21	9	In XeroSecurity Sn1per 9.0 (free version), insecure permissions (0777) are set upon application execution, allowing an unprivileged user to modify the application, modules, and configuration files. This leads to arbitrary code execution with root privileges. **CVE ID : CVE-2021-39273**	N/A	A-XER-SN1P-020921/376
Incorrect Default Permissions	19-Aug-21	10	In XeroSecurity Sn1per 9.0 (free version), insecure directory permissions (0777) are set during installation, allowing an unprivileged user to modify the main application and the application configuration file. This results in arbitrary code execution with root privileges. **CVE ID : CVE-2021-39274**	N/A	A-XER-SN1P-020921/377
xstream_project					
xstream					
Deserialization of Untrusted	23-Aug-21	6.5	XStream is a simple library to serialize objects to XML and back again. In affected versions	https://github.com/x-stream/xstre	A-XST-XSTR-020921/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Data			this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. A user is only affected if using the version out of the box with JDK 1.7u21 or below. However, this scenario can be adjusted easily to an external Xalan that works regardless of the version of the Java runtime. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose. **CVE ID : CVE-2021-39139**	am/security/advisories/GHSA-64xx-cq4q-mf44, https://x-stream.github.io/CVE-2021-39139.html	
Deserialization of Untrusted Data	23-Aug-21	6.5	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general	https://x-stream.github.io/CVE-2021-39141.html, https://github.com/x-stream/xstream/security/advisories/GHSA-g5w6-mrj7-75h2	A-XST-XSTR-020921/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			purpose. **CVE ID : CVE-2021-39141**		
Improper Control of Generation of Code ('Code Injection')	23-Aug-21	6.5	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker has sufficient rights to execute commands of the host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose. **CVE ID : CVE-2021-39144**	https://x-stream.github.io/CVE-2021-39144.html, https://github.com/x-stream/xstream/security/advisories/GHSA-j9h8-phrw-h4fh	A-XST-XSTR-020921/380
Unrestricted Upload of File with Dangerous Type	23-Aug-21	6	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose. **CVE ID : CVE-2021-39145**	https://x-stream.github.io/CVE-2021-39145.html, https://github.com/x-stream/xstream/security/advisories/GHSA-8jrj-525p-826v	A-XST-XSTR-020921/381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	23-Aug-21	6	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose. **CVE ID : CVE-2021-39146**	https://github.com/x-stream/xstream/security/advisories/GHSA-p8pq-r894-fm8f, https://x-stream.github.io/CVE-2021-39146.html	A-XST-XSTR-020921/382
Yandex					
clickhouse					
N/A	17-Aug-21	4	Clickhouse prior to versions v20.8.18.32-lts, v21.1.9.41-stable, v21.2.9.41-stable, v21.3.6.55-lts, v21.4.3.21-stable allows user to read any file on the host system, that clickhouse user has access to. **CVE ID : CVE-2021-25263**	https://clickhouse.tech/docs/en/whats-new/security-changelog/	A-YAN-CLIC-020921/383
yclas					
yclas					
Improper Neutralization of Input During Web Page Generation ('Cross-site	18-Aug-21	4.3	Static (Persistent) XSS Vulnerability exists in version 4.3.0 of Yclas when using the install/view/form.php script. An attacker can store XSS in the database through the vulnerable SITE_NAME	N/A	A-YCL-YCLA-020921/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			parameter. **CVE ID : CVE-2021-38710**		
youtube_embed_project					
youtube_embed					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-21	2.1	The YouTube Embed WordPress plugin before 5.2.2 does not validate, escape or sanitise some of its shortcode attributes, leading to Stored XSS issues by 1. using w, h, controls, cc_lang, color, language, start, stop, or style parameter of youtube shortcode, 2. by using style, class, rel, target, width, height, or alt parameter of youtube_thumb shortcode, or 3. by embedding a video whose title or description contains XSS payload (if API key is configured). **CVE ID : CVE-2021-24471**	N/A	A-YOU-YOUT-020921/385
zint					
barcode_generator					
Out-of-bounds Read	17-Aug-21	4.3	Zint Barcode Generator before 2.10.0 has a one-byte buffer over-read, related to is_last_single_ascii in code1.c, and rs_encode_uint in reedsol.c. **CVE ID : CVE-2021-39247**	https://sourceforge.net/p/zint/code/ci/9b02cd52214e80f945bff41fc94bc1e17e15810c/, https://sourceforge.net/p/zint/tickets/232/	A-ZIN-BARC-020921/386
zstack					
rest_api					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	17-Aug-21	6.5	ZStack is open source IaaS(infrastructure as a service) software aiming to automate datacenters, managing resources of compute, storage, and networking all by APIs. Affected versions of ZStack REST API are vulnerable to post-authentication Remote Code Execution (RCE) via bypass of the Groovy shell sandbox. The REST API exposes the GET zstack/v1/batch-queries?script endpoint which is backed up by the BatchQueryAction class. Messages are represented by the APIBatchQueryMsg, dispatched to the QueryFacadeImpl facade and handled by the BatchQuery class. The HTTP request parameter script is mapped to the APIBatchQueryMsg.script property and evaluated as a Groovy script in BatchQuery.query the evaluation of the user-controlled Groovy script is sandboxed by SandboxTransformer which will apply the restrictions defined in the registered (sandbox.register()) GroovyInterceptor. Even though the sandbox heavily restricts the receiver types to a small set of allowed types, the sandbox is non effective at	https://securitylab.github.com/advisories/GHSL-2021-065-zstack/	A-ZST-REST-020921/387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controlling any code placed in Java annotations and therefore vulnerable to meta-programming escapes. This issue leads to post-authenticated remote code execution. For more details see the referenced GHSL-2021-065. This issue is patched in versions 3.8.21, 3.10.8, and 4.1.0. **CVE ID : CVE-2021-32829**		
Hardware					
altus					
hadron_xtorm_hx3040					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	H-ALT-HADR-020921/388
Improper Neutralization of Special Elements	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and	https://www.altus.com.br/	H-ALT-HADR-020921/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	H-ALT-HADR-020921/390
nexto_nx3003					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	H-ALT-NEXT-020921/391
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040	https://www.altus.com.br/	H-ALT-NEXT-020921/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	H-ALT-NEXT-020921/393
nexto_nx3004					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325	https://www.altus.com.br/	H-ALT-NEXT-020921/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	H-ALT-NEXT-020921/395
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto	https://www.altus.com.br/	H-ALT-NEXT-020921/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**		
nexto_nx3005					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	H-ALT-NEXT-020921/397
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100	https://www.altus.com.br/	H-ALT-NEXT-020921/398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	H-ALT-NEXT-020921/399
nexto_nx3010					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto	https://www.altus.com.br/	H-ALT-NEXT-020921/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	H-ALT-NEXT-020921/401
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004	https://www.altus.com.br/	H-ALT-NEXT-020921/402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**		
nexto_nx3020					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	H-ALT-NEXT-020921/403
Improper Neutralization of Special Elements	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and	https://www.altus.com.br/	H-ALT-NEXT-020921/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	H-ALT-NEXT-020921/405
nexto_nx3030					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	H-ALT-NEXT-020921/406
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040	https://www.altus.com.br/	H-ALT-NEXT-020921/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	H-ALT-NEXT-020921/408
nexto_nx5100					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325	https://www.altus.com.br/	H-ALT-NEXT-020921/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	H-ALT-NEXT-020921/410
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto	https://www.altus.com.br/	H-ALT-NEXT-020921/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**		
nexto_nx5101					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	H-ALT-NEXT-020921/412
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100	https://www.altus.com.br/	H-ALT-NEXT-020921/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	H-ALT-NEXT-020921/414
nexto_nx5110					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto	https://www.altus.com.br/	H-ALT-NEXT-020921/415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	H-ALT-NEXT-020921/416
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004	https://www.altus.com.br/	H-ALT-NEXT-020921/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**		
nexto_nx5210					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	H-ALT-NEXT-020921/418
Improper Neutralization of Special Elements	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and	https://www.altus.com.br/	H-ALT-NEXT-020921/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	H-ALT-NEXT-020921/420
nexto_xpress_xp300					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	H-ALT-NEXT-020921/421
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040	https://www.altus.com.br/	H-ALT-NEXT-020921/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	H-ALT-NEXT-020921/423
nexto_xpress_xp315					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325	https://www.altus.com.br/	H-ALT-NEXT-020921/424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	H-ALT-NEXT-020921/425
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto	https://www.altus.com.br/	H-ALT-NEXT-020921/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**		
nexto_xpress_xp325					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	H-ALT-NEXT-020921/427
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100	https://www.altus.com.br/	H-ALT-NEXT-020921/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	H-ALT-NEXT-020921/429
nexto_xpress_xp340					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto	https://www.altus.com.br/	H-ALT-NEXT-020921/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	H-ALT-NEXT-020921/431
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004	https://www.altus.com.br/	H-ALT-NEXT-020921/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**		
ARM					
china_star-mc1					
Incorrect Authorization	23-Aug-21	3.6	Certain Arm products before 2021-08-23 do not properly consider the effect of exceptions on a VLLDM instruction. A Non-secure handler may have read or write access to part of a Secure context. This affects Arm Cortex-M33 r0p0 through r1p0, Arm Cortex-M35P r0, Arm Cortex-M55 r0p0 through r1p0, and Arm China STAR-MC1 (in the STAR SE configuration). **CVE ID : CVE-2021-35465**	https://developer.arm.com/support/arm-security-updates/vlldm-instruction-security-vulnerability, https://developer.arm.com/support/arm-security-updates	H-ARM-CHIN-020921/433
cortex-35p					
Incorrect Authorization	23-Aug-21	3.6	Certain Arm products before 2021-08-23 do not properly consider the effect of exceptions on a VLLDM instruction. A Non-secure handler may have read or write access to part of a Secure	https://developer.arm.com/support/arm-security-updates/vlldm-instruction-	H-ARM-CORT-020921/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			context. This affects Arm Cortex-M33 r0p0 through r1p0, Arm Cortex-M35P r0, Arm Cortex-M55 r0p0 through r1p0, and Arm China STAR-MC1 (in the STAR SE configuration). **CVE ID : CVE-2021-35465**	security-vulnerability, https://developer.arm.com/support/arm-security-updates	
cortex-m33					
Incorrect Authorization	23-Aug-21	3.6	Certain Arm products before 2021-08-23 do not properly consider the effect of exceptions on a VLLDM instruction. A Non-secure handler may have read or write access to part of a Secure context. This affects Arm Cortex-M33 r0p0 through r1p0, Arm Cortex-M35P r0, Arm Cortex-M55 r0p0 through r1p0, and Arm China STAR-MC1 (in the STAR SE configuration). **CVE ID : CVE-2021-35465**	https://developer.arm.com/support/arm-security-updates/vlldm-instruction-security-vulnerability, https://developer.arm.com/support/arm-security-updates	H-ARM-CORT-020921/435
cortex-m55					
Incorrect Authorization	23-Aug-21	3.6	Certain Arm products before 2021-08-23 do not properly consider the effect of exceptions on a VLLDM instruction. A Non-secure handler may have read or write access to part of a Secure context. This affects Arm Cortex-M33 r0p0 through r1p0, Arm Cortex-M35P r0, Arm Cortex-M55 r0p0 through r1p0, and Arm China STAR-MC1 (in the STAR SE configuration).	https://developer.arm.com/support/arm-security-updates/vlldm-instruction-security-vulnerability, https://developer.arm.com/support/arm-security-updates	H-ARM-CORT-020921/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35465		
Cisco					
rv110w_wireless-n_vpn_firewall					
Improper Input Validation	18-Aug-21	10	A vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of incoming UPnP traffic. An attacker could exploit this vulnerability by sending a crafted UPnP request to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a DoS condition. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-34730**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-sb-rv-overflow-htpymMB5	H-CIS-RV11-020921/437
rv130w_wireless-n_multifunction_vpn_router					
Improper Input Validation	18-Aug-21	10	A vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-sb-	H-CIS-RV13-020921/438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of incoming UPnP traffic. An attacker could exploit this vulnerability by sending a crafted UPnP request to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a DoS condition. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-34730**	rv-overflow-htpymMB5	
rv130_vpn_router					
Improper Input Validation	18-Aug-21	10	A vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of incoming UPnP traffic. An attacker could exploit this vulnerability by sending a crafted UPnP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-sb-rv-overflow-htpymMB5	H-CIS-RV13-020921/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a DoS condition. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-34730**		
rv215w_wireless-n_vpn_router					
Improper Input Validation	18-Aug-21	10	A vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of incoming UPnP traffic. An attacker could exploit this vulnerability by sending a crafted UPnP request to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a DoS condition. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-34730**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-sb-rv-overflow-htpymMB5	H-CIS-RV21-020921/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
secure_email_and_web_manager					
Improper Authentication	18-Aug-21	5.5	A vulnerability in the spam quarantine feature of Cisco Secure Email and Web Manager, formerly Cisco Security Management Appliance (SMA), could allow an authenticated, remote attacker to gain unauthorized access and modify the spam quarantine settings of another user. This vulnerability exists because access to the spam quarantine feature is not properly restricted. An attacker could exploit this vulnerability by sending malicious requests to an affected system. A successful exploit could allow the attacker to modify another user's spam quarantine settings, possibly disabling security controls or viewing email messages stored on the spam quarantine interfaces. **CVE ID : CVE-2021-1561**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-spam-jPxUXMk	H-CIS-SECU-020921/441
cyberoamworks					
netgenie_c0101b1-20141120-ng11vo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-21	4.3	Cyberoam NetGenie C0101B1-20141120-NG11VO devices through 2021-08-14 allow tweb/ft.php?u=[XSS] attacks. **CVE ID : CVE-2021-38702**	http://www.cyberoamworks.com/NetGenie-Home.asp	H-CYB-NETG-020921/442
D-link					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dcs-2750u					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Aug-21	7.2	D-Link router DSL-2750U with firmware vME1.16 or prior versions is vulnerable to OS command injection. An unauthenticated attacker on the local network may exploit this, with CVE-2021-3707, to execute any OS commands on the vulnerable device. **CVE ID : CVE-2021-3708**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10230	H-D-L-DCS--020921/443
dsl-2750u					
Missing Authorization	16-Aug-21	2.1	D-Link router DSL-2750U with firmware vME1.16 or prior versions is vulnerable to unauthorized configuration modification. An unauthenticated attacker on the local network may exploit this, with CVE-2021-3708, to execute any OS commands on the vulnerable device. **CVE ID : CVE-2021-3707**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10230	H-D-L-DSL--020921/444
Dlink					
dsr-500n					
Use of Hard-coded Credentials	23-Aug-21	10	** UNSUPPORTED WHEN ASSIGNED ** D-Link DSR-500N version 1.02 contains hard-coded credentials for undocumented user accounts in the '/etc/passwd' file.If an attacker succeeds in recovering the cleartext password of the identified hash value, he will be able to log in via SSH or Telnet and thus gain access to the underlying embedded Linux	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10235	H-DLI-DSR--020921/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system on the device. Fixed in version 2.12/2. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-39615**		
dvg-3104ms					
Use of Hard-coded Credentials	23-Aug-21	5	** UNSUPPORTED WHEN ASSIGNED ** D-Link DVG-3104MS version 1.0.2.0.3, 1.0.2.0.4, and 1.0.2.0.4E contains hard-coded credentials for undocumented user accounts in the '/etc/passwd' file. As weak passwords have been used, the plaintext passwords can be recovered from the hash values. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-39613**	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10237	H-DLI-DVG--020921/446
dvx-2000ms					
Use of Hard-coded Credentials	23-Aug-21	5	D-Link DVX-2000MS contains hard-coded credentials for undocumented user accounts in the '/etc/passwd' file. As weak passwords have been used, the plaintext passwords can be recovered from the hash values. **CVE ID : CVE-2021-39614**	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10236	H-DLI-DVX--020921/447
Huawei					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
cloudengine_12800					
Improper Handling of Exceptional Conditions	23-Aug-21	5	There is a denial of service vulnerability in some huawei products. In specific scenarios, due to the improper handling of the packets, an attacker may craft the specific packet. Successful exploit may cause some services abnormal. Affected product versions include:CloudEngine 12800 V200R005C00SPC800, CloudEngine 5800 V200R005C00SPC800, CloudEngine 6800 V200R005C00SPC800, CloudEngine 7800 V200R005C00SPC800. **CVE ID : CVE-2021-22328**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210407-01-dos-en	H-HUA-CLOU-020921/448
cloudengine_5800					
Improper Handling of Exceptional Conditions	23-Aug-21	5	There is a denial of service vulnerability in some huawei products. In specific scenarios, due to the improper handling of the packets, an attacker may craft the specific packet. Successful exploit may cause some services abnormal. Affected product versions include:CloudEngine 12800 V200R005C00SPC800, CloudEngine 5800 V200R005C00SPC800, CloudEngine 6800 V200R005C00SPC800, CloudEngine 7800 V200R005C00SPC800. **CVE ID : CVE-2021-22328**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210407-01-dos-en	H-HUA-CLOU-020921/449
cloudengine_6800					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	23-Aug-21	5	There is a denial of service vulnerability in some huawei products. In specific scenarios, due to the improper handling of the packets, an attacker may craft the specific packet. Successful exploit may cause some services abnormal. Affected product versions include:CloudEngine 12800 V200R005C00SPC800, CloudEngine 5800 V200R005C00SPC800, CloudEngine 6800 V200R005C00SPC800, CloudEngine 7800 V200R005C00SPC800. **CVE ID : CVE-2021-22328**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210407-01-dos-en	H-HUA-CLOU-020921/450
cloudengine_7800					
Improper Handling of Exceptional Conditions	23-Aug-21	5	There is a denial of service vulnerability in some huawei products. In specific scenarios, due to the improper handling of the packets, an attacker may craft the specific packet. Successful exploit may cause some services abnormal. Affected product versions include:CloudEngine 12800 V200R005C00SPC800, CloudEngine 5800 V200R005C00SPC800, CloudEngine 6800 V200R005C00SPC800, CloudEngine 7800 V200R005C00SPC800. **CVE ID : CVE-2021-22328**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210407-01-dos-en	H-HUA-CLOU-020921/451
s12700					
Improper	23-Aug-21	5	There is a denial of service	https://www	H-HUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability in Huawei products. A module cannot deal with specific messages due to validating inputs insufficiently. Attackers can exploit this vulnerability by sending specific messages to affected module. This can cause denial of service. Affected product versions include: S12700 V200R013C00SPC500, V200R019C00SPC500; S5700 V200R013C00SPC500, V200R019C00SPC500; S6700 V200R013C00SPC500, V200R019C00SPC500; S7700 V200R013C00SPC500, V200R019C00SPC500. **CVE ID : CVE-2021-22357**	.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-dos-en	S127-020921/452
s5700					
Improper Input Validation	23-Aug-21	5	There is a denial of service vulnerability in Huawei products. A module cannot deal with specific messages due to validating inputs insufficiently. Attackers can exploit this vulnerability by sending specific messages to affected module. This can cause denial of service. Affected product versions include: S12700 V200R013C00SPC500, V200R019C00SPC500; S5700 V200R013C00SPC500, V200R019C00SPC500; S6700 V200R013C00SPC500, V200R019C00SPC500; S7700 V200R013C00SPC500,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-dos-en	H-HUA-S570-020921/453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R019C00SPC500. **CVE ID : CVE-2021-22357**		
s6700					
Improper Input Validation	23-Aug-21	5	There is a denial of service vulnerability in Huawei products. A module cannot deal with specific messages due to validating inputs insufficiently. Attackers can exploit this vulnerability by sending specific messages to affected module. This can cause denial of service. Affected product versions include: S12700 V200R013C00SPC500, V200R019C00SPC500; S5700 V200R013C00SPC500, V200R019C00SPC500; S6700 V200R013C00SPC500, V200R019C00SPC500; S7700 V200R013C00SPC500, V200R019C00SPC500. **CVE ID : CVE-2021-22357**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-dos-en	H-HUA-S670-020921/454
s7700					
Improper Input Validation	23-Aug-21	5	There is a denial of service vulnerability in Huawei products. A module cannot deal with specific messages due to validating inputs insufficiently. Attackers can exploit this vulnerability by sending specific messages to affected module. This can cause denial of service. Affected product versions include: S12700 V200R013C00SPC500, V200R019C00SPC500; S5700	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-dos-en	H-HUA-S770-020921/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R013C00SPC500, V200R019C00SPC500; S6700 V200R013C00SPC500, V200R019C00SPC500; S7700 V200R013C00SPC500, V200R019C00SPC500. **CVE ID : CVE-2021-22357**		
Lenovo					
smart_camera_c2e					
Improper Control of Generation of Code ('Code Injection')	17-Aug-21	4.6	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow code execution if a specific file exists on the attached SD card. This vulnerability is the same as CNVD-2021-45262. **CVE ID : CVE-2021-3615**	https://iknow.lenovo.com.cn/detail/dc_198417.html	H-LEN-SMAR-020921/456
N/A	17-Aug-21	7.5	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow an unauthorized user to view device information, alter firmware content and device configuration. This vulnerability is the same as CNVD-2020-68651. **CVE ID : CVE-2021-3616**	https://iknow.lenovo.com.cn/detail/dc_198417.html	H-LEN-SMAR-020921/457
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Aug-21	6.5	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow command injection by setting a specially crafted network configuration. This vulnerability is the same as CNVD-2020-68652. **CVE ID : CVE-2021-3617**	https://iknow.lenovo.com.cn/detail/dc_198417.html	H-LEN-SMAR-020921/458
smart_camera_x3					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	17-Aug-21	4.6	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow code execution if a specific file exists on the attached SD card. This vulnerability is the same as CNVD-2021-45262. **CVE ID : CVE-2021-3615**	https://iknow.lenovo.com.cn/detail/dc_198417.html	H-LEN-SMAR-020921/459
N/A	17-Aug-21	7.5	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow an unauthorized user to view device information, alter firmware content and device configuration. This vulnerability is the same as CNVD-2020-68651. **CVE ID : CVE-2021-3616**	https://iknow.lenovo.com.cn/detail/dc_198417.html	H-LEN-SMAR-020921/460
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Aug-21	6.5	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow command injection by setting a specially crafted network configuration. This vulnerability is the same as CNVD-2020-68652. **CVE ID : CVE-2021-3617**	https://iknow.lenovo.com.cn/detail/dc_198417.html	H-LEN-SMAR-020921/461
smart_camera_x5					
Improper Control of Generation of Code ('Code Injection')	17-Aug-21	4.6	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow code execution if a specific file exists on the attached SD card. This vulnerability is the same as CNVD-2021-45262. **CVE ID : CVE-2021-3615**	https://iknow.lenovo.com.cn/detail/dc_198417.html	H-LEN-SMAR-020921/462
N/A	17-Aug-21	7.5	A vulnerability was reported in Lenovo Smart Camera X3, X5,	https://iknow.lenovo.co	H-LEN-SMAR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and C2E that could allow an unauthorized user to view device information, alter firmware content and device configuration. This vulnerability is the same as CNVD-2020-68651. **CVE ID : CVE-2021-3616**	m.cn/detail/dc_198417.html	020921/463
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Aug-21	6.5	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow command injection by setting a specially crafted network configuration. This vulnerability is the same as CNVD-2020-68652. **CVE ID : CVE-2021-3617**	https://iknow.lenovo.com.cn/detail/dc_198417.html	H-LEN-SMAR-020921/464
Motorola					
mm1000					
Improper Authentication	17-Aug-21	2.1	The Motorola MM1000 device configuration portal can be accessed without authentication, which could allow adapter settings to be modified. **CVE ID : CVE-2021-3458**	https://motorolamentor.zendesk.com/hc/en-us/articles/12608040477 50	H-MOT-MM10-020921/465
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-21	7.2	A privilege escalation vulnerability was reported in the MM1000 device configuration web server, which could allow privileged shell access and/or arbitrary privileged commands to be executed on the adapter. **CVE ID : CVE-2021-3459**	https://motorolamentor.zendesk.com/hc/en-us/articles/12608040477 50	H-MOT-MM10-020921/466
netmodule					
nb1600					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	H-NET-NB16-020921/467
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB16-020921/468
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB16-020921/469
nb1601					
Insecure	23-Aug-21	5	Certain NetModule devices	http://seclist	H-NET-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Storage of Sensitive Information			have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	s.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	NB16-020921/470
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB16-020921/471
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB16-020921/472
nb1800					
Insecure Storage of	23-Aug-21	5	Certain NetModule devices have Insecure Password	http://seclists.org/fulldisc	H-NET-NB18-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	losure/2021/Aug/22, https://www.netmodule.com	020921/473
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB18-020921/474
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB18-020921/475
nb1810					
Insecure Storage of Sensitive	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or	http://seclists.org/fulldisclosure/2021	H-NET-NB18-020921/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	/Aug/22, https://www.netmodule.com	
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB18-020921/477
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB18-020921/478
nb2700					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These	http://seclists.org/fulldisclosure/2021/Aug/22,	H-NET-NB27-020921/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	https://www.netmodule.com	
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB27-020921/480
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB27-020921/481
nb2710					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before	http://seclists.org/fulldisclosure/2021/Aug/22, https://www	H-NET-NB27-020921/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	.netmodule.com	
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB27-020921/483
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB27-020921/484
nb2800					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.c	H-NET-NB28-020921/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	om	
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB28-020921/486
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB28-020921/487
nb2810					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800,	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	H-NET-NB28-020921/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**		
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB28-020921/489
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB28-020921/490
nb3700					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800,	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	H-NET-NB37-020921/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**		
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB37-020921/492
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB37-020921/493
nb3701					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710,	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	H-NET-NB37-020921/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**		
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB37-020921/495
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB37-020921/496
nb3710					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700,	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	H-NET-NB37-020921/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**		
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB37-020921/498
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB37-020921/499
nb3711					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711,	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	H-NET-NB37-020921/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NB3720, and NB3800. **CVE ID : CVE-2021-39289**		
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB37-020921/501
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB37-020921/502
nb3720					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800.	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	H-NET-NB37-020921/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39289		
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB37-020921/504
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB37-020921/505
nb3800					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	H-NET-NB38-020921/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	H-NET-NB38-020921/507
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB38-020921/508
nb800					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	H-NET-NB80-020921/509
Session	23-Aug-21	7.5	Certain NetModule devices	https://www	H-NET-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Fixation			allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	.netmodule.com	NB80-020921/510
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	H-NET-NB80-020921/511
Siemens					
sentron_3wa_com190					
Improper Input Validation	19-Aug-21	5	An issue was discovered in tcp_rcv() in nptcp.c in HCC embedded InterNiche 4.0.1. The TCP header processing code doesn't sanitize the value of the IP total length field (header length + data length). With a crafted IP packet, an integer overflow occurs whenever the value of the IP data length is calculated by subtracting the length of the header from the total length of the IP packet.	https://cert-portal.siemens.com/productcert/pdf/ssa-789208.pdf	H-SIE-SENT-020921/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31401		
sentron_3wl_com35					
Improper Input Validation	19-Aug-21	5	An issue was discovered in tcp_rcv() in nptcp.c in HCC embedded InterNiche 4.0.1. The TCP header processing code doesn't sanitize the value of the IP total length field (header length + data length). With a crafted IP packet, an integer overflow occurs whenever the value of the IP data length is calculated by subtracting the length of the header from the total length of the IP packet. **CVE ID : CVE-2021-31401**	https://cert-portal.siemens.com/productcert/pdf/ssa-789208.pdf	H-SIE-SENT-020921/513
totolink					
a3002r					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-21	4.3	Cross-site scripting in ddns.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "Domain Name" field, "Server Address" field, "User Name/Email", or "Password/Key" field. **CVE ID : CVE-2021-34207**	N/A	H-TOT-A300-020921/514
Improper Neutralization of Input During Web Page Generation ('Cross-site	20-Aug-21	4.3	Cross-site scripting in tcpipwan.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the	N/A	H-TOT-A300-020921/515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			"Service Name" field. **CVE ID : CVE-2021-34215**		
N/A	20-Aug-21	5	Directory Indexing in Login Portal of Login Portal of TOTOLINK-A702R-V1.0.0-B20161227.1023 allows attacker to access /add/ , /img/, /js/, and /mobile directories via GET Parameter. **CVE ID : CVE-2021-34218**	N/A	H-TOT-A300-020921/516
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-21	4.3	Cross-site scripting in tr069config.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "User Name" field or "Password" field. **CVE ID : CVE-2021-34220**	N/A	H-TOT-A300-020921/517
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-21	4.3	Cross-site scripting in urlfilter.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "URL Address" field. **CVE ID : CVE-2021-34223**	N/A	H-TOT-A300-020921/518
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-21	4.3	Cross-site scripting in parent_control.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "Description" field and "Service Name" field.	N/A	H-TOT-A300-020921/519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34228		
Tp-link					
tl-wr840n					
Exposure of Resource to Wrong Sphere	19-Aug-21	4.3	In TP-Link Wireless N Router WR840N an ARP poisoning attack can cause buffer overflow **CVE ID : CVE-2021-29280**	N/A	H-TP--TL-W-020921/520
Operating System					
altus					
hadron_xtorm_hx3040_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	O-ALT-HADR-020921/521
Improper Neutralization of Special Elements used in an OS Command ('OS	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003	https://www.altus.com.br/	O-ALT-HADR-020921/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	O-ALT-HADR-020921/523
nexto_nx3003_firmware					
Cross-Site Request Forgery	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron	https://www.altus.com.br/	O-ALT-NEXT-020921/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	O-ALT-NEXT-020921/525
Use of Hard-	23-Aug-21	5	Hardcoded .htaccess	https://www	O-ALT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	.altus.com.br/	NEXT-020921/526
nexto_nx3004_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	O-ALT-NEXT-020921/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	O-ALT-NEXT-020921/528
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040	https://www.altus.com.br/	O-ALT-NEXT-020921/529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.7.58.0. **CVE ID : CVE-2021-39245**		
nexto_nx3005_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	O-ALT-NEXT-020921/530
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto	https://www.altus.com.br/	O-ALT-NEXT-020921/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	O-ALT-NEXT-020921/532
nexto_nx3010_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto	https://www.altus.com.br/	O-ALT-NEXT-020921/533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	O-ALT-NEXT-020921/534
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100	https://www.altus.com.br/	O-ALT-NEXT-020921/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**		
nexto_nx3020_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	O-ALT-NEXT-020921/536
Improper Neutralization of Special Elements used in an OS Command ('OS Command	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004	https://www.altus.com.br/	O-ALT-NEXT-020921/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	O-ALT-NEXT-020921/538
nexto_nx3030_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI	https://www.altus.com.br/	O-ALT-NEXT-020921/539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	O-ALT-NEXT-020921/540
Use of Hard-coded	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist	https://www.altus.com.br	O-ALT-NEXT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	/	020921/541
nexto_nx5100_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	O-ALT-NEXT-020921/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	O-ALT-NEXT-020921/543
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040	https://www.altus.com.br/	O-ALT-NEXT-020921/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.7.58.0. **CVE ID : CVE-2021-39245**		
nexto_nx5101_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	O-ALT-NEXT-020921/545
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto	https://www.altus.com.br/	O-ALT-NEXT-020921/546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	O-ALT-NEXT-020921/547
nexto_nx5110_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto	https://www.altus.com.br/	O-ALT-NEXT-020921/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	O-ALT-NEXT-020921/549
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100	https://www.altus.com.br/	O-ALT-NEXT-020921/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**		
nexto_nx5210_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	O-ALT-NEXT-020921/551
Improper Neutralization of Special Elements used in an OS Command ('OS Command	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004	https://www.altus.com.br/	O-ALT-NEXT-020921/552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	O-ALT-NEXT-020921/553
nexto_xpress_xp300_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI	https://www.altus.com.br/	O-ALT-NEXT-020921/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	O-ALT-NEXT-020921/555
Use of Hard-coded	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist	https://www.altus.com.br	O-ALT-NEXT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	/	020921/556
nexto_xpress_xp315_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	O-ALT-NEXT-020921/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	O-ALT-NEXT-020921/558
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040	https://www.altus.com.br/	O-ALT-NEXT-020921/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.7.58.0. **CVE ID : CVE-2021-39245**		
nexto_xpress_xp325_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**	https://www.altus.com.br/	O-ALT-NEXT-020921/560
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto	https://www.altus.com.br/	O-ALT-NEXT-020921/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**		
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**	https://www.altus.com.br/	O-ALT-NEXT-020921/562
nexto_xpress_xp340_firmware					
Cross-Site Request Forgery (CSRF)	23-Aug-21	4.3	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto	https://www.altus.com.br/	O-ALT-NEXT-020921/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39243**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Aug-21	9	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39244**	https://www.altus.com.br/	O-ALT-NEXT-020921/564
Use of Hard-coded Credentials	23-Aug-21	5	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100	https://www.altus.com.br/	O-ALT-NEXT-020921/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0. **CVE ID : CVE-2021-39245**		
Apple					
macos					
Uncontrolled Search Path Element	20-Aug-21	9.3	Adobe Dimension version 3.4 (and earlier) is affected by an Uncontrolled Search Path Element element. 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-2021-28595**	https://helpx.adobe.com/security/products/dimension/apsb21-40.html	O-APP-MACO-020921/566
Stack-based Buffer Overflow	20-Aug-21	9.3	Adobe Photoshop versions 21.2.9 (and earlier) and 22.4.2 (and earlier) is affected by a stack overflow vulnerability due to insecure handling of a crafted PSD file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted PSD file in Photoshop. **CVE ID : CVE-2021-36005**	https://helpx.adobe.com/security/products/photoshop/apsb21-63.html	O-APP-MACO-020921/567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Aug-21	4.3	Adobe Photoshop versions 21.2.9 (and earlier) and 22.4.2 (and earlier) are affected by an Improper input validation 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-2021-36006**	https://helpx.adobe.com/security/products/photoshop/apsb21-63.html	O-APP-MACO-020921/568
mac_os					
N/A	23-Aug-21	4	A Denial-of-Service (DoS) vulnerability was discovered in all versions of F-Secure Atlant whereby the SAVAPI component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33598**	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	O-APP-MAC_-020921/569
ARM					
china_star-mc1_firmware					
Incorrect Authorization	23-Aug-21	3.6	Certain Arm products before 2021-08-23 do not properly consider the effect of exceptions on a VLLDM	https://developer.arm.com/support/arm-security-	O-ARM-CHIN-020921/570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			instruction. A Non-secure handler may have read or write access to part of a Secure context. This affects Arm Cortex-M33 r0p0 through r1p0, Arm Cortex-M35P r0, Arm Cortex-M55 r0p0 through r1p0, and Arm China STAR-MC1 (in the STAR SE configuration). **CVE ID : CVE-2021-35465**	updates/vlldm-instruction-security-vulnerability, https://developer.arm.com/support/arm-security-updates	
cortex-35p_firmware					
Incorrect Authorization	23-Aug-21	3.6	Certain Arm products before 2021-08-23 do not properly consider the effect of exceptions on a VLLDM instruction. A Non-secure handler may have read or write access to part of a Secure context. This affects Arm Cortex-M33 r0p0 through r1p0, Arm Cortex-M35P r0, Arm Cortex-M55 r0p0 through r1p0, and Arm China STAR-MC1 (in the STAR SE configuration). **CVE ID : CVE-2021-35465**	https://developer.arm.com/support/arm-security-updates/vlldm-instruction-security-vulnerability, https://developer.arm.com/support/arm-security-updates	O-ARM-CORT-020921/571
cortex-m33_firmware					
Incorrect Authorization	23-Aug-21	3.6	Certain Arm products before 2021-08-23 do not properly consider the effect of exceptions on a VLLDM instruction. A Non-secure handler may have read or write access to part of a Secure context. This affects Arm Cortex-M33 r0p0 through r1p0, Arm Cortex-M35P r0, Arm Cortex-M55 r0p0 through	https://developer.arm.com/support/arm-security-updates/vlldm-instruction-security-vulnerability, https://developer.arm.co	O-ARM-CORT-020921/572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			r1p0, and Arm China STAR-MC1 (in the STAR SE configuration). **CVE ID : CVE-2021-35465**	m/support/arm-security-updates	
cortex-m55_firmware					
Incorrect Authorization	23-Aug-21	3.6	Certain Arm products before 2021-08-23 do not properly consider the effect of exceptions on a VLLDM instruction. A Non-secure handler may have read or write access to part of a Secure context. This affects Arm Cortex-M33 r0p0 through r1p0, Arm Cortex-M35P r0, Arm Cortex-M55 r0p0 through r1p0, and Arm China STAR-MC1 (in the STAR SE configuration). **CVE ID : CVE-2021-35465**	https://developer.arm.com/support/arm-security-updates/vlldm-instruction-security-vulnerability, https://developer.arm.com/support/arm-security-updates	O-ARM-CORT-020921/573
Blackberry					
qnx_os_for_medical					
Integer Overflow or Wraparound	17-Aug-21	6.8	An integer overflow vulnerability in the calloc() function of the C runtime library of affected versions of BlackBerry® QNX Software Development Platform (SDP) version(s) 6.5.0SP1 and earlier, QNX OS for Medical 1.1 and earlier, and QNX OS for Safety 1.0.1 and earlier that could allow an attacker to potentially perform a denial of service or execute arbitrary code. **CVE ID : CVE-2021-22156**	https://support.blackberry.com/kb/articleDetail?articleNumber=000082334	O-BLA-QNX_-020921/574
qnx_os_for_safety					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	17-Aug-21	6.8	An integer overflow vulnerability in the calloc() function of the C runtime library of affected versions of BlackBerry® QNX Software Development Platform (SDP) version(s) 6.5.0SP1 and earlier, QNX OS for Medical 1.1 and earlier, and QNX OS for Safety 1.0.1 and earlier that could allow an attacker to potentially perform a denial of service or execute arbitrary code. **CVE ID : CVE-2021-22156**	https://support.blackberry.com/kb/articleDetail?articleNumber=000082334	O-BLA-QNX_-020921/575
Cisco					
firepower_management_center_virtual_appliance_firmware					
Exposure of Sensitive Information to an Unauthorized Actor	18-Aug-21	5	A vulnerability in Server Name Identification (SNI) request filtering of Cisco Web Security Appliance (WSA), Cisco Firepower Threat Defense (FTD), and the Snort detection engine could allow an unauthenticated, remote attacker to bypass filtering technology on an affected device and exfiltrate data from a compromised host. This vulnerability is due to inadequate filtering of the SSL handshake. An attacker could exploit this vulnerability by using data from the SSL client hello packet to communicate with an external server. A successful exploit could allow the attacker to execute a command-and-control attack on a compromised host and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sni-data-exfil-mFgzXqLN	O-CIS-FIRE-020921/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			perform additional data exfiltration attacks. **CVE ID : CVE-2021-34749**		
rv110w_wireless-n_vpn_firewall_firmware					
Improper Input Validation	18-Aug-21	10	A vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of incoming UPnP traffic. An attacker could exploit this vulnerability by sending a crafted UPnP request to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a DoS condition. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-34730**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-sb-rv-overflow-htpymMB5	O-CIS-RV11-020921/577
rv130w_wireless-n_multifunction_vpn_router_firmware					
Improper Input Validation	18-Aug-21	10	A vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-RV13-020921/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of incoming UPnP traffic. An attacker could exploit this vulnerability by sending a crafted UPnP request to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a DoS condition. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-34730**	sa-cisco-sb-rv-overflow-htpymMB5	
rv130_vpn_router_firmware					
Improper Input Validation	18-Aug-21	10	A vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of incoming UPnP traffic. An attacker could exploit this vulnerability by sending a crafted UPnP request to an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-sb-rv-overflow-htpymMB5	O-CIS-RV13-020921/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a DoS condition. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-34730**		
rv215w_wireless-n_vpn_router_firmware					
Improper Input Validation	18-Aug-21	10	A vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of incoming UPnP traffic. An attacker could exploit this vulnerability by sending a crafted UPnP request to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a DoS condition. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-34730**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-sb-rv-overflow-htpymMB5	O-CIS-RV21-020921/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
secure_email_and_web_manager					
Improper Authentication	18-Aug-21	5.5	A vulnerability in the spam quarantine feature of Cisco Secure Email and Web Manager, formerly Cisco Security Management Appliance (SMA), could allow an authenticated, remote attacker to gain unauthorized access and modify the spam quarantine settings of another user. This vulnerability exists because access to the spam quarantine feature is not properly restricted. An attacker could exploit this vulnerability by sending malicious requests to an affected system. A successful exploit could allow the attacker to modify another user's spam quarantine settings, possibly disabling security controls or viewing email messages stored on the spam quarantine interfaces. **CVE ID : CVE-2021-1561**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-spam-jPxUXMk	O-CIS-SECU-020921/581
video_surveillance_7000_ip_camera_firmware					
Double Free	18-Aug-21	6.1	A vulnerability in the Link Layer Discovery Protocol (LLDP) implementation for the Cisco Video Surveillance 7000 Series IP Cameras firmware could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper management of memory resources, referred to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-dos-OFP7j9j	O-CIS-VIDE-020921/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as a double free. An attacker could exploit this vulnerability by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-34734**		
cyberoamworks					
netgenie_c0101b1-20141120-ng11vo_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-21	4.3	Cyberoam NetGenie C0101B1-20141120-NG11VO devices through 2021-08-14 allow tweb/ft.php?u=[XSS] attacks. **CVE ID : CVE-2021-38702**	http://www.cyberoamworks.com/NetGenie-Home.asp	O-CYB-NETG-020921/583
D-link					
dcs-2750u_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Aug-21	7.2	D-Link router DSL-2750U with firmware vME1.16 or prior versions is vulnerable to OS command injection. An unauthenticated attacker on the local network may exploit this, with CVE-2021-3707, to execute any OS commands on the vulnerable device. **CVE ID : CVE-2021-3708**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10230	O-D-L-DCS--020921/584
dsl-2750u_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	16-Aug-21	2.1	D-Link router DSL-2750U with firmware vME1.16 or prior versions is vulnerable to unauthorized configuration modification. An unauthenticated attacker on the local network may exploit this, with CVE-2021-3708, to execute any OS commands on the vulnerable device. **CVE ID : CVE-2021-3707**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10230	O-D-L-DSL--020921/585
Debian					
debian_linux					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	6.8	LedgerSMB does not check the origin of HTML fragments merged into the browser's DOM. By sending a specially crafted URL to an authenticated user, this flaw can be abused for remote code execution and information disclosure. **CVE ID : CVE-2021-3693**	https://ledgersmb.org/cve-2021-3693-cross-site-scripting, https://huntr.dev/bounties/daf1384d-648a-43fd-9b35-5c37d8ead667	O-DEB-DEBI-020921/586
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-21	6.8	LedgerSMB does not sufficiently HTML-encode error messages sent to the browser. By sending a specially crafted URL to an authenticated user, this flaw can be abused for remote code execution and information disclosure. **CVE ID : CVE-2021-3694**	https://huntr.dev/bounties/ef7f4cf7-3a81-4516-b261-f5b6ac21430c, https://ledgersmb.org/cve-2021-3694-cross-site-scripting, https://github.com/ledger	O-DEB-DEBI-020921/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				smb/ledgersmb/commit/98fa476d46a4a7e5e9492ed69b4fa190be5547fc	
Improper Restriction of Rendered UI Layers or Frames	23-Aug-21	4.3	LedgerSMB does not sufficiently guard against being wrapped by other sites, making it vulnerable to 'clickjacking'. This allows an attacker to trick a targetted user to execute unintended actions. **CVE ID : CVE-2021-3731**	https://hunter.dev/bounties/5664331d-f5f8-4412-8566-408f8655888a, https://ledgersmb.org/cve-2021-3731-clickjacking	O-DEB-DEBI-020921/588
N/A	17-Aug-21	5	An issue was discovered in HAProxy 2.2 before 2.2.16, 2.3 before 2.3.13, and 2.4 before 2.4.3. It does not ensure that the scheme and path portions of a URI have the expected characters. For example, the authority field (as observed on a target HTTP/2 server) might differ from what the routing rules were intended to achieve. **CVE ID : CVE-2021-39240**	https://git.haproxy.org/?p=haproxy.git;a=commit;h=a495e0d94876c9d39763db319f609351907a31e8, https://git.haproxy.org/?p=haproxy.git;a=commit;h=4b8852c70d8c4b7e225e24eb58258a15eb54c26e	O-DEB-DEBI-020921/589
N/A	17-Aug-21	5	An issue was discovered in HAProxy 2.0 before 2.0.24, 2.2 before 2.2.16, 2.3 before 2.3.13, and 2.4 before 2.4.3. An HTTP method name may contain a space followed by the name of a protected resource.	https://git.haproxy.org/?p=haproxy.git;a=commit;h=89265224d314a056d77d974284802c	O-DEB-DEBI-020921/590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			It is possible that a server would interpret this as a request for that protected resource, such as in the "GET /admin? HTTP/1.1 /static/images HTTP/1.1" example. **CVE ID : CVE-2021-39241**	1b8a0dc97f	
Improper Handling of Exceptional Conditions	17-Aug-21	5	An issue was discovered in HAProxy 2.2 before 2.2.16, 2.3 before 2.3.13, and 2.4 before 2.4.3. It can lead to a situation with an attacker-controlled HTTP Host header, because a mismatch between Host and authority is mishandled. **CVE ID : CVE-2021-39242**	https://git.haproxy.org/?p=haproxy.git;a=commit;h=b5d2b9e154d78e4075db163826c5e0f6d31b2ab1	O-DEB-DEBI-020921/591
Improper Certificate Validation	22-Aug-21	4.3	In GNOME grilo though 0.3.13, grl-net-wc.c does not enable TLS certificate verification on the SoupSessionAsync objects it creates, leaving users vulnerable to network MITM attacks. NOTE: this is similar to CVE-2016-20011. **CVE ID : CVE-2021-39365**	https://gitlab.gnome.org/GNOME/grilo/-/issues/146, https://blogs.gnome.org/mcatanzaro/2021/05/25/reminder-soupsessionsync-and-soupsessionasync-default-to-no-tls-certificate-verification/	O-DEB-DEBI-020921/592
Dell					
emc_powerscale_onefs					
Improper Privilege	16-Aug-21	4	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.x contain an insufficient logging	https://www.dell.com/support/kbdoc/	O-DEL-EMC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			vulnerability. An authenticated user with ISI_PRIV_LOGIN_PAPI could make un-audited and un-trackable configuration changes to settings that their roles have privileges to change. **CVE ID : CVE-2021-21568**	000190408	020921/593
Improper Handling of Exceptional Conditions	16-Aug-21	4	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.x improperly handle an exceptional condition. A remote low privileged user could potentially exploit this vulnerability, leading to unauthorized information disclosure. **CVE ID : CVE-2021-21592**	https://www.dell.com/support/kbdoc/000190408	O-DEL-EMC_-020921/594
Use of GET Request Method With Sensitive Query Strings	16-Aug-21	5	Dell PowerScale OneFS versions 8.2.2 - 9.1.0.x contain a use of get request method with sensitive query strings vulnerability. It can lead to potential disclosure of sensitive data. Dell recommends upgrading at your earliest opportunity. **CVE ID : CVE-2021-21594**	https://www.dell.com/support/kbdoc/000190408	O-DEL-EMC_-020921/595
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Aug-21	4.6	Dell EMC PowerScale OneFS versions 8.2.x - 9.1.1.x contain an improper neutralization of special elements used in an OS command. This vulnerability could allow the compadmin user to elevate privileges. This only impacts Smartlock WORM compliance mode clusters as a critical vulnerability and Dell recommends to	https://www.dell.com/support/kbdoc/000190408	O-DEL-EMC_-020921/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update/upgrade at the earliest opportunity. **CVE ID : CVE-2021-21595**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Aug-21	4.6	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.1.x contain an OS command injection vulnerability. This may allow a user with ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE to escalate privileges and escape the compliance guarantees. This only impacts Smartlock WORM compliance mode clusters as a critical vulnerability and Dell recommends to update/upgrade at the earliest opportunity. **CVE ID : CVE-2021-21599**	https://www.dell.com/support/kbdoc/000190408	O-DEL-EMC_-020921/597
Insertion of Sensitive Information into Log File	16-Aug-21	2.1	Dell EMC PowerScale OneFS versions 8.2.x and 9.1.0.x contain an insertion of sensitive information into log files vulnerability. This means a malicious actor with ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE privileges can access privileged information. **CVE ID : CVE-2021-36278**	https://www.dell.com/support/kbdoc/000190408	O-DEL-EMC_-020921/598
Incorrect Permission Assignment for Critical Resource	16-Aug-21	7.2	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.x contain an incorrect permission assignment for critical resource vulnerability. This could allow a user with ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE to access privileged information	https://www.dell.com/support/kbdoc/000190408	O-DEL-EMC_-020921/599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			about the cluster. **CVE ID : CVE-2021-36279**		
Incorrect Permission Assignment for Critical Resource	16-Aug-21	2.1	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.x contain an incorrect permission assignment for critical resource vulnerability. This could allow a user with ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE to access privileged information about the cluster. **CVE ID : CVE-2021-36280**	https://www.dell.com/support/kbdoc/000190408	O-DEL-EMC_-020921/600
Incorrect Permission Assignment for Critical Resource	16-Aug-21	6.5	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.x contain an incorrect permission assignment vulnerability. A low privileged authenticated user can potentially exploit this vulnerability to escalate privileges. **CVE ID : CVE-2021-36281**	https://www.dell.com/support/kbdoc/000190408	O-DEL-EMC_-020921/601
Improper Handling of Exceptional Conditions	16-Aug-21	2.1	Dell EMC PowerScale OneFS versions 8.2.x - 9.1.0.x contain a use of uninitialized resource vulnerability. This can potentially allow an authenticated user with ISI_PRIV_LOGIN_CONSOLE or ISI_PRIV_LOGIN_SSH privileges to gain access up to 24 bytes of data within the /ifs kernel stack under certain conditions. **CVE ID : CVE-2021-36282**	https://www.dell.com/support/kbdoc/000190408	O-DEL-EMC_-020921/602
Dlink					
dsr-500n_firmware					
Use of Hard-coded	23-Aug-21	10	** UNSUPPORTED WHEN ASSIGNED ** D-Link DSR-500N	https://www.dlink.com/e	O-DLI-DSR--020921/603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			version 1.02 contains hard-coded credentials for undocumented user accounts in the '/etc/passwd' file.If an attacker succeeds in recovering the cleartext password of the identified hash value, he will be able to log in via SSH or Telnet and thus gain access to the underlying embedded Linux operating system on the device. Fixed in version 2.12/2. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-39615**	n/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10235	
dvg-3104ms_firmware					
Use of Hard-coded Credentials	23-Aug-21	5	** UNSUPPORTED WHEN ASSIGNED ** D-Link DVG-3104MS version 1.0.2.0.3, 1.0.2.0.4, and 1.0.2.0.4E contains hard-coded credentials for undocumented user accounts in the '/etc/passwd' file. As weak passwords have been used, the plaintext passwords can be recovered from the hash values. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-39613**	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10237	O-DLI-DVG--020921/604
dvx-2000ms_firmware					
Use of Hard-coded Credentials	23-Aug-21	5	D-Link DVX-2000MS contains hard-coded credentials for undocumented user accounts	https://www.dlink.com/en/security-	O-DLI-DVX--020921/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the '/etc/passwd' file. As weak passwords have been used, the plaintext passwords can be recovered from the hash values. **CVE ID : CVE-2021-39614**	bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10236	
Fedoraproject					
fedora					
Reachable Assertion	18-Aug-21	5	In BIND 9.16.19, 9.17.16. Also, version 9.16.19-S1 of BIND Supported Preview Edition When a vulnerable version of named receives a query under the circumstances described above, the named process will terminate due to a failed assertion check. The vulnerability affects only BIND 9 releases 9.16.19, 9.17.16, and release 9.16.19-S1 of the BIND Supported Preview Edition. **CVE ID : CVE-2021-25218**	https://kb.isc.org/v1/docs/cve-2021-25218, http://www.openwall.com/lists/oss-security/2021/08/18/3, http://www.openwall.com/lists/oss-security/2021/08/20/2	O-FED-FEDO-020921/606
NULL Pointer Dereference	23-Aug-21	4	The Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.18.5 and 1.19.x before 1.19.3 has a NULL pointer dereference in kdc/do_tgs_req.c via a FAST inner body that lacks a server field. **CVE ID : CVE-2021-37750**	https://web.mit.edu/kerberos/advisories/, https://github.com/krb5/krb5/commit/d775c95af7606a51bf79547a94fa52ddd1cb7f49	O-FED-FEDO-020921/607
Google					
android					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Aug-21	4.6	In clk driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05479659; Issue ID: ALPS05479659. **CVE ID : CVE-2021-0407**	N/A	O-GOO-ANDR-020921/608
Out-of-bounds Read	18-Aug-21	2.1	In asf extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489195; Issue ID: ALPS05489220. **CVE ID : CVE-2021-0408**	N/A	O-GOO-ANDR-020921/609
Incorrect Authorization	18-Aug-21	2.1	In memory management driver, 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: ALPS05403499; Issue ID: ALPS05336692. **CVE ID : CVE-2021-0415**	N/A	O-GOO-ANDR-020921/610
Improper Input Validation	18-Aug-21	4.9	In memory management driver, there is a possible system crash due to improper input validation. This could lead to local denial of service	N/A	O-GOO-ANDR-020921/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05336700. **CVE ID : CVE-2021-0416**		
Improper Input Validation	18-Aug-21	4.9	In memory management driver, there is a possible system crash due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05336702. **CVE ID : CVE-2021-0417**	N/A	O-GOO-ANDR-020921/612
Improper Input Validation	18-Aug-21	4.9	In memory management driver, there is a possible system crash due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05336706. **CVE ID : CVE-2021-0418**	N/A	O-GOO-ANDR-020921/613
Improper Input Validation	18-Aug-21	4.9	In memory management driver, there is a possible system crash due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	N/A	O-GOO-ANDR-020921/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05336713. **CVE ID : CVE-2021-0419**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Aug-21	4.9	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381065. **CVE ID : CVE-2021-0420**	N/A	O-GOO-ANDR-020921/615
Out-of-bounds Write	17-Aug-21	7.2	In BITSTREAM_FLUSH of ih264e_bitstream.h, there is a possible out of bounds write 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.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-176533109 **CVE ID : CVE-2021-0519**	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/616
Out-of-bounds Write	17-Aug-21	4.6	In asf extractor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187231635 **CVE ID : CVE-2021-0573**		
Out-of-bounds Write	17-Aug-21	4.6	In asf extractor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187234876 **CVE ID : CVE-2021-0574**	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/618
Out-of-bounds Write	17-Aug-21	4.6	In flv extractor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187236084 **CVE ID : CVE-2021-0576**	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/619
Out-of-bounds Read	17-Aug-21	3.3	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SoCAndroid ID: A-187161772 **CVE ID : CVE-2021-0578**		
Out-of-bounds Read	17-Aug-21	3.3	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187231636 **CVE ID : CVE-2021-0579**	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/621
Out-of-bounds Read	17-Aug-21	3.3	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187231637 **CVE ID : CVE-2021-0580**	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/622
Out-of-bounds Read	17-Aug-21	3.3	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SoCAndroid ID: A-187231638 **CVE ID : CVE-2021-0581**		
Out-of-bounds Read	17-Aug-21	3.3	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187149601 **CVE ID : CVE-2021-0582**	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/624
Out-of-bounds Read	17-Aug-21	2.1	In verifyBufferObject of Parcel.cpp, there is a possible out of bounds read due to an improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-179289794 **CVE ID : CVE-2021-0584**	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/625
Externally Controlled Reference to a Resource in Another Sphere	17-Aug-21	6.8	In sendReplyIntentToReceiver of BluetoothPermissionActivity.java, there is a possible way to invoke privileged broadcast receivers due to a confused deputy. This could lead to local escalation of privilege with User execution privileges	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-179386960 **CVE ID : CVE-2021-0591**		
Externally Controlled Reference to a Resource in Another Sphere	17-Aug-21	4.6	In sendDevicePickedIntent of DevicePickerFragment.java, there is a possible way to invoke a privileged broadcast receiver due to a confused deputy. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-179386068 **CVE ID : CVE-2021-0593**	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/627
Out-of-bounds Write	18-Aug-21	4.6	In ged, 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: ALPS05687510; Issue ID: ALPS05687510. **CVE ID : CVE-2021-0626**	N/A	O-GOO-ANDR-020921/628
Integer Overflow or Wraparound	18-Aug-21	4.6	In OMA DRM, there is a possible memory corruption due to an integer overflow. This could lead to local	N/A	O-GOO-ANDR-020921/629

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: ALPS05722434; Issue ID: ALPS05722434. **CVE ID : CVE-2021-0627**		
Improper Input Validation	18-Aug-21	4.6	In OMA DRM, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05722454; Issue ID: ALPS05722454. **CVE ID : CVE-2021-0628**	N/A	O-GOO-ANDR-020921/630
Insecure Storage of Sensitive Information	17-Aug-21	2.1	In multiple functions of libl3oemcrypto.cpp, there is a possible weakness in the existing obfuscation mechanism due to the way sensitive data is handled. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-190724551 **CVE ID : CVE-2021-0639**	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/631
Out-of-bounds Write	17-Aug-21	4.6	In noteAtomLogged of StatsdStats.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-187957589 **CVE ID : CVE-2021-0640**		
Missing Authorization	17-Aug-21	2.1	In getAvailableSubscriptionInfoList of SubscriptionController.java, there is a possible disclosure of unique identifiers 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.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-185235454 **CVE ID : CVE-2021-0641**	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/633
Missing Authorization	17-Aug-21	4.3	In onResume of VoicemailSettingsFragment.java, there is a possible way to retrieve a trackable identifier without permissions due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-185126149	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0642		
Improper Privilege Management	17-Aug-21	6.8	In shouldBlockFromTree of ExternalStorageProvider.java, there is a possible permissions bypass. This could lead to local escalation of privilege, allowing an app to read private app directories in external storage, which should be restricted in Android 11, with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157320644 **CVE ID : CVE-2021-0645**	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/635
Improper Input Validation	17-Aug-21	4.6	In sqlite3_str_vappendf of sqlite3.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege if the user can also inject a printf into a privileged process's SQL with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-153352319 **CVE ID : CVE-2021-0646**	https://source.android.com/security/bulletin/2021-08-01	O-GOO-ANDR-020921/636
N/A	17-Aug-21	4.3	Firefox for Android could get stuck in fullscreen mode and not exit it even after normal interactions that should cause it to exit. *Note: This issue only	https://www.mozilla.org/security/advisories/mfsa2021-33/,	O-GOO-ANDR-020921/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 91. **CVE ID : CVE-2021-29983**	https://bugzilla.mozilla.org/show_bug.cgi?id=1719088	
Origin Validation Error	26-Aug-21	4.3	Incorrect security UI in Navigation in Google Chrome on Android prior to 92.0.4515.131 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-30596**	https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html, https://crbug.com/1214481	O-GOO-ANDR-020921/638
Huawei					
cloudengine_12800_firmware					
Improper Handling of Exceptional Conditions	23-Aug-21	5	There is a denial of service vulnerability in some huawei products. In specific scenarios, due to the improper handling of the packets, an attacker may craft the specific packet. Successful exploit may cause some services abnormal. Affected product versions include:CloudEngine 12800 V200R005C00SPC800, CloudEngine 5800 V200R005C00SPC800, CloudEngine 6800 V200R005C00SPC800, CloudEngine 7800 V200R005C00SPC800. **CVE ID : CVE-2021-22328**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210407-01-dos-en	O-HUA-CLOU-020921/639
cloudengine_5800_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	23-Aug-21	5	There is a denial of service vulnerability in some huawei products. In specific scenarios, due to the improper handling of the packets, an attacker may craft the specific packet. Successful exploit may cause some services abnormal. Affected product versions include:CloudEngine 12800 V200R005C00SPC800, CloudEngine 5800 V200R005C00SPC800, CloudEngine 6800 V200R005C00SPC800, CloudEngine 7800 V200R005C00SPC800. **CVE ID : CVE-2021-22328**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210407-01-dos-en	O-HUA-CLOU-020921/640
cloudengine_6800_firmware					
Improper Handling of Exceptional Conditions	23-Aug-21	5	There is a denial of service vulnerability in some huawei products. In specific scenarios, due to the improper handling of the packets, an attacker may craft the specific packet. Successful exploit may cause some services abnormal. Affected product versions include:CloudEngine 12800 V200R005C00SPC800, CloudEngine 5800 V200R005C00SPC800, CloudEngine 6800 V200R005C00SPC800, CloudEngine 7800 V200R005C00SPC800. **CVE ID : CVE-2021-22328**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210407-01-dos-en	O-HUA-CLOU-020921/641
cloudengine_7800_firmware					
Improper	23-Aug-21	5	There is a denial of service	https://www	O-HUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Handling of Exceptional Conditions			vulnerability in some huawei products. In specific scenarios, due to the improper handling of the packets, an attacker may craft the specific packet. Successful exploit may cause some services abnormal. Affected product versions include:CloudEngine 12800 V200R005C00SPC800, CloudEngine 5800 V200R005C00SPC800, CloudEngine 6800 V200R005C00SPC800, CloudEngine 7800 V200R005C00SPC800. **CVE ID : CVE-2021-22328**	.huawei.com/en/psirt/security-advisories/huawei-sa-20210407-01-dos-en	CLOU-020921/642
s12700_firmware					
Improper Input Validation	23-Aug-21	5	There is a denial of service vulnerability in Huawei products. A module cannot deal with specific messages due to validating inputs insufficiently. Attackers can exploit this vulnerability by sending specific messages to affected module. This can cause denial of service. Affected product versions include: S12700 V200R013C00SPC500, V200R019C00SPC500; S5700 V200R013C00SPC500, V200R019C00SPC500; S6700 V200R013C00SPC500, V200R019C00SPC500; S7700 V200R013C00SPC500, V200R019C00SPC500. **CVE ID : CVE-2021-22357**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-dos-en	O-HUA-S127-020921/643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
s5700_firmware					
Improper Input Validation	23-Aug-21	5	There is a denial of service vulnerability in Huawei products. A module cannot deal with specific messages due to validating inputs insufficiently. Attackers can exploit this vulnerability by sending specific messages to affected module. This can cause denial of service. Affected product versions include: S12700 V200R013C00SPC500, V200R019C00SPC500; S5700 V200R013C00SPC500, V200R019C00SPC500; S6700 V200R013C00SPC500, V200R019C00SPC500; S7700 V200R013C00SPC500, V200R019C00SPC500. **CVE ID : CVE-2021-22357**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-dos-en	O-HUA-S570-020921/644
s6700_firmware					
Improper Input Validation	23-Aug-21	5	There is a denial of service vulnerability in Huawei products. A module cannot deal with specific messages due to validating inputs insufficiently. Attackers can exploit this vulnerability by sending specific messages to affected module. This can cause denial of service. Affected product versions include: S12700 V200R013C00SPC500, V200R019C00SPC500; S5700 V200R013C00SPC500, V200R019C00SPC500; S6700 V200R013C00SPC500,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-dos-en	O-HUA-S670-020921/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R019C00SPC500; S7700 V200R013C00SPC500, V200R019C00SPC500. **CVE ID : CVE-2021-22357**		
s7700_firmware					
Improper Input Validation	23-Aug-21	5	There is a denial of service vulnerability in Huawei products. A module cannot deal with specific messages due to validating inputs insufficiently. Attackers can exploit this vulnerability by sending specific messages to affected module. This can cause denial of service. Affected product versions include: S12700 V200R013C00SPC500, V200R019C00SPC500; S5700 V200R013C00SPC500, V200R019C00SPC500; S6700 V200R013C00SPC500, V200R019C00SPC500; S7700 V200R013C00SPC500, V200R019C00SPC500. **CVE ID : CVE-2021-22357**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210512-01-dos-en	O-HUA-S770-020921/646
Juniper					
junos					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Aug-21	7.8	A buffer overflow vulnerability in the TCP/IP stack of Juniper Networks Junos OS allows an attacker to send specific sequences of packets to the device thereby causing a Denial of Service (DoS). By repeatedly sending these sequences of packets to the device, an attacker can sustain the Denial of Service (DoS)	https://kb.juniper.net/JSA11200	O-JUN-JUNO-020921/647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. The device will abnormally shut down as a result of these sent packets. A potential indicator of compromise will be the following message in the log files: "eventd[13955]: SYSTEM_ABNORMAL_SHUTDOWN: System abnormally shut down" This issue is only triggered by traffic destined to the device. Transit traffic will not trigger this issue. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S19; 15.1 versions prior to 15.1R7-S10; 17.3 versions prior to 17.3R3-S12; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2; 21.2 versions prior to 21.2R2. **CVE ID : CVE-2021-0284**		
Lenovo					
smart_camera_c2e_firmware					
Improper Control of Generation of Code ('Code	17-Aug-21	4.6	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow code execution if a specific file exists on the attached SD card. This	https://iknow.lenovo.com.cn/detail/dc_198417.ht	O-LEN-SMAR-020921/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			vulnerability is the same as CNVD-2021-45262. **CVE ID : CVE-2021-3615**	ml	
N/A	17-Aug-21	7.5	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow an unauthorized user to view device information, alter firmware content and device configuration. This vulnerability is the same as CNVD-2020-68651. **CVE ID : CVE-2021-3616**	https://iknow.lenovo.com.cn/detail/dc_198417.html	O-LEN-SMAR-020921/649
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Aug-21	6.5	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow command injection by setting a specially crafted network configuration. This vulnerability is the same as CNVD-2020-68652. **CVE ID : CVE-2021-3617**	https://iknow.lenovo.com.cn/detail/dc_198417.html	O-LEN-SMAR-020921/650
smart_camera_x3_firmware					
Improper Control of Generation of Code ('Code Injection')	17-Aug-21	4.6	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow code execution if a specific file exists on the attached SD card. This vulnerability is the same as CNVD-2021-45262. **CVE ID : CVE-2021-3615**	https://iknow.lenovo.com.cn/detail/dc_198417.html	O-LEN-SMAR-020921/651
N/A	17-Aug-21	7.5	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow an unauthorized user to view device information, alter firmware content and device configuration. This	https://iknow.lenovo.com.cn/detail/dc_198417.html	O-LEN-SMAR-020921/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is the same as CNVD-2020-68651. **CVE ID : CVE-2021-3616**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Aug-21	6.5	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow command injection by setting a specially crafted network configuration. This vulnerability is the same as CNVD-2020-68652. **CVE ID : CVE-2021-3617**	https://iknow.lenovo.com.cn/detail/dc_198417.html	O-LEN-SMAR-020921/653
smart_camera_x5_firmware					
Improper Control of Generation of Code ('Code Injection')	17-Aug-21	4.6	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow code execution if a specific file exists on the attached SD card. This vulnerability is the same as CNVD-2021-45262. **CVE ID : CVE-2021-3615**	https://iknow.lenovo.com.cn/detail/dc_198417.html	O-LEN-SMAR-020921/654
N/A	17-Aug-21	7.5	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow an unauthorized user to view device information, alter firmware content and device configuration. This vulnerability is the same as CNVD-2020-68651. **CVE ID : CVE-2021-3616**	https://iknow.lenovo.com.cn/detail/dc_198417.html	O-LEN-SMAR-020921/655
Improper Neutralization of Special Elements used in a Command ('Command	17-Aug-21	6.5	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow command injection by setting a specially crafted network configuration. This vulnerability is the same as	https://iknow.lenovo.com.cn/detail/dc_198417.html	O-LEN-SMAR-020921/656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			CNVD-2020-68652. **CVE ID : CVE-2021-3617**		
Linux					
linux_kernel					
Use of Uninitialized Resource	18-Aug-21	2.1	An information disclosure vulnerability exists in the ARM SIGPAGE functionality of Linux Kernel v5.4.66 and v5.4.54. The latest version (5.11-rc4) seems to still be vulnerable. A userland application can read the contents of the sigpage, which can leak kernel memory contents. An attacker can read a process's memory at a specific offset to trigger this vulnerability. This was fixed in kernel releases: 4.14.222 4.19.177 5.4.99 5.10.17 5.11 **CVE ID : CVE-2021-21781**	N/A	O-LIN-LINU-020921/657
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Aug-21	6.8	A suspected race condition when calling getaddrinfo led to memory corruption and a potentially exploitable crash. *Note: This issue only affected Linux operating systems. Other operating systems are unaffected.* This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91. **CVE ID : CVE-2021-29986**	https://www.mozilla.org/security/advisories/mfsa2021-34/, https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://www.mozilla.org/security/advisories/mfsa2	O-LIN-LINU-020921/658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				021-35/	
Improper Restriction of Excessive Authenticati on Attempts	17-Aug-21	4.3	After requesting multiple permissions, and closing the first permission panel, subsequent permission panels will be displayed in a different position but still record a click in the default location, making it possible to trick a user into accepting a permission they did not want to. *This bug only affects Firefox on Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox < 91 and Thunderbird < 91. **CVE ID : CVE-2021-29987**	https://www.mozilla.org/security/advisories/mfsa2021-33/, https://www.mozilla.org/security/advisories/mfsa2021-36/, https://bugzilla.mozilla.org/show_bug.cgi?id=1716129	O-LIN-LINU-020921/659
Cleartext Storage of Sensitive Information	18-Aug-21	5	In Octopus Server after version 2018.8.2 if the Octopus Server Web Request Proxy is configured with authentication, the password is shown in plaintext in the UI. **CVE ID : CVE-2021-31820**	https://advisories.octopus.com/adv/2021-07---Proxy-Password-Stored-in-Plaintext-(CVE-2021-31820).2193063986.html	O-LIN-LINU-020921/660
Microsoft					
windows					
Out-of-bounds Read	20-Aug-21	6.8	Adobe Media Encoder version 15.2 (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 achieve arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/media-encoder/apsb21-43.html	O-MIC-WIND-020921/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-28589**		
Out-of-bounds Read	20-Aug-21	6.8	Adobe Media Encoder version 15.2 (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 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-2021-28590**	https://helpx.adobe.com/security/products/media-encoder/apsb21-43.html	O-MIC-WIND-020921/662
Out-of-bounds Write	20-Aug-21	6.8	Adobe Illustrator version 25.2.3 (and earlier) is affected by an Out-of-bounds Write 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-2021-28591**	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	O-MIC-WIND-020921/663
Out-of-bounds Write	20-Aug-21	6.8	Adobe Illustrator version 25.2.3 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a specially crafted file. An unauthenticated attacker could	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	O-MIC-WIND-020921/664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2021-28592**		
Use After Free	20-Aug-21	4.3	Adobe Illustrator version 25.2.3 (and earlier) is affected by a Use After Free vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose potential sensitive 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-2021-28593**	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	O-MIC-WIND-020921/665
Uncontrolled Search Path Element	20-Aug-21	9.3	Adobe Dimension version 3.4 (and earlier) is affected by an Uncontrolled Search Path Element element. 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-2021-28595**	https://helpx.adobe.com/security/products/dimension/apsb21-40.html	O-MIC-WIND-020921/666
Out-of-bounds Write	23-Aug-21	9.3	Adobe Framemaker version 2020.0.1 (and earlier) and 2019.0.8 (and earlier) are affected by an Out-of-bounds	https://helpx.adobe.com/security/products/framem	O-MIC-WIND-020921/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Write 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-2021-28596**	aker/apsb21-45.html	
Out-of-bounds Read	24-Aug-21	5.8	Adobe After Effects version 18.2 (and earlier) is affected by an Our-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information and cause a 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-2021-28612**	https://helpx.adobe.com/security/products/after_effects/apsb21-49.html	O-MIC-WIND-020921/668
Out-of-bounds Read	24-Aug-21	5.8	Adobe After Effects version 18.2 (and earlier) is affected by an Our-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information and cause a denial of service in the context of the current user. Exploitation of this issue requires user interaction in that a victim	https://helpx.adobe.com/security/products/after_effects/apsb21-49.html	O-MIC-WIND-020921/669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must open a malicious file. **CVE ID : CVE-2021-28614**		
Out-of-bounds Read	24-Aug-21	4.3	Adobe Animate version 21.0.6 (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 sensitive 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-2021-28619**	https://helpx.adobe.com/security/products/animate/apsb21-50.html	O-MIC-WIND-020921/670
Heap-based Buffer Overflow	24-Aug-21	6.8	Adobe Animate version 21.0.6 (and earlier) is affected by a Heap-based Buffer Overflow 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-2021-28620**	https://helpx.adobe.com/security/products/animate/apsb21-50.html	O-MIC-WIND-020921/671
Out-of-bounds Read	24-Aug-21	6.8	Adobe Animate version 21.0.6 (and earlier) is affected by an Out-of-bounds Read 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	https://helpx.adobe.com/security/products/animate/apsb21-50.html	O-MIC-WIND-020921/672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-28621**		
Out-of-bounds Write	24-Aug-21	6.8	Adobe Animate version 21.0.6 (and earlier) is affected by an Out-of-bounds Write 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-2021-28622**	https://helpx.adobe.com/security/products/animate/apsb21-50.html	O-MIC-WIND-020921/673
Heap-based Buffer Overflow	20-Aug-21	9.3	Adobe Bridge version 11.0.2 (and earlier) are affected by a Heap-based Buffer overflow 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-2021-28624**	https://helpx.adobe.com/security/products/bridge/apsb21-53.html	O-MIC-WIND-020921/674
Heap-based Buffer Overflow	24-Aug-21	6.8	Adobe Animate version 21.0.6 (and earlier) is affected by a Heap-based Buffer Overflow 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	https://helpx.adobe.com/security/products/animate/apsb21-50.html	O-MIC-WIND-020921/675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-28629**		
Out-of-bounds Read	24-Aug-21	6.8	Adobe Animate version 21.0.6 (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 potential sensitive 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-2021-28630**	https://helpx.adobe.com/security/products/animate/apsb21-50.html	O-MIC-WIND-020921/676
Cleartext Storage of Sensitive Information	18-Aug-21	5	In Octopus Server after version 2018.8.2 if the Octopus Server Web Request Proxy is configured with authentication, the password is shown in plaintext in the UI. **CVE ID : CVE-2021-31820**	https://advisories.octopus.com/adv/2021-07---Proxy-Password-Stored-in-Plaintext-(CVE-2021-31820).2193063986.html	O-MIC-WIND-020921/677
N/A	23-Aug-21	4	A Denial-of-Service (DoS) vulnerability was discovered in all versions of F-Secure Atlant whereby the SAVAPI component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-	O-MIC-WIND-020921/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Anti-Virus engine. **CVE ID : CVE-2021-33598**	secure.com/en/business/support-and-downloads/security-advisories	
Out-of-bounds Write	20-Aug-21	9.3	Adobe Bridge version 11.0.2 (and earlier) is affected by an Out-of-bounds Write 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-2021-35989**	https://helpx.adobe.com/security/products/bridge/apsb21-53.html	O-MIC-WIND-020921/679
Out-of-bounds Write	20-Aug-21	9.3	Adobe Bridge version 11.0.2 (and earlier) is affected by an Out-of-bounds Write 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-2021-35990**	https://helpx.adobe.com/security/products/bridge/apsb21-53.html	O-MIC-WIND-020921/680
Improper Input Validation	20-Aug-21	4.3	Adobe Bridge version 11.0.2 (and earlier) is affected by an uninitialized variable vulnerability when parsing a specially crafted file. An	https://helpx.adobe.com/security/products/bridge/apsb21-	O-MIC-WIND-020921/681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2021-35991**	53.html	
Out-of-bounds Read	20-Aug-21	4.3	Adobe Bridge version 11.0.2 (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 sensitive 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-2021-35992**	https://helpx.adobe.com/security/products/bridge/apsb21-53.html	O-MIC-WIND-020921/682
Access of Memory Location After End of Buffer	20-Aug-21	9.3	Adobe Premiere Pro version 15.2 (and earlier) is affected by a memory corruption 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-2021-35997**	https://helpx.adobe.com/security/products/premiere_pro/apsb21-56.html	O-MIC-WIND-020921/683
Access of Memory	20-Aug-21	9.3	Adobe Prelude version 10.0 (and earlier) is affected by a	https://helpx.adobe.com/s	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Location After End of Buffer			memory corruption 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-2021-35999**	ecurity/products/prelude/apsb21-58.html	020921/684
Access of Memory Location After End of Buffer	20-Aug-21	9.3	Adobe Character Animator version 4.2 (and earlier) is affected by a memory corruption 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-2021-36000**	https://helpx.adobe.com/in/security/products/character_animator/apsb21-59.html	O-MIC-WIND-020921/685
Out-of-bounds Read	20-Aug-21	4.3	Adobe Character Animator version 4.2 (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	https://helpx.adobe.com/in/security/products/character_animator/apsb21-59.html	O-MIC-WIND-020921/686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious file. **CVE ID : CVE-2021-36001**		
Stack-based Buffer Overflow	20-Aug-21	9.3	Adobe Photoshop versions 21.2.9 (and earlier) and 22.4.2 (and earlier) is affected by a stack overflow vulnerability due to insecure handling of a crafted PSD file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted PSD file in Photoshop. **CVE ID : CVE-2021-36005**	https://helpx.adobe.com/security/products/photoshop/apsb21-63.html	O-MIC-WIND-020921/687
Improper Input Validation	20-Aug-21	4.3	Adobe Photoshop versions 21.2.9 (and earlier) and 22.4.2 (and earlier) are affected by an Improper input validation 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-2021-36006**	https://helpx.adobe.com/security/products/photoshop/apsb21-63.html	O-MIC-WIND-020921/688
Use of Uninitialized Resource	20-Aug-21	6.8	Adobe Prelude version 10.0 (and earlier) are affected by an uninitialized variable vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose arbitrary memory information in the context of	https://helpx.adobe.com/security/products/prelude/apsb21-58.html	O-MIC-WIND-020921/689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-36007**		
Use After Free	20-Aug-21	4.3	Adobe Illustrator version 25.2.3 (and earlier) is affected by an Use-after-free vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to read arbitrary file system 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-2021-36008**	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	O-MIC-WIND-020921/690
Access of Memory Location After End of Buffer	20-Aug-21	9.3	Adobe Illustrator version 25.2.3 (and earlier) is affected by an memory corruption 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-2021-36009**	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	O-MIC-WIND-020921/691
Out-of-bounds Read	20-Aug-21	4.3	Adobe Illustrator version 25.2.3 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of memory. An attacker could leverage this	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	O-MIC-WIND-020921/692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2021-36010**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Aug-21	9.3	Adobe Illustrator version 25.2.3 (and earlier) is affected by a potential Command injection vulnerability when chained with a development and debugging tool for JavaScript scripts. 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-2021-36011**	https://helpx.adobe.com/security/products/illustrator/apsb21-42.html	O-MIC-WIND-020921/693
Access of Uninitialized Pointer	20-Aug-21	4.3	Adobe Media Encoder version 15.2 (and earlier) is affected by an uninitialized pointer vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to read arbitrary file system 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-2021-36014**	https://helpx.adobe.com/security/products/media-encoder/apsb21-43.html	O-MIC-WIND-020921/694
Access of Memory	20-Aug-21	9.3	Adobe Media Encoder version 15.2 (and earlier) is affected by	https://helpx.adobe.com/s	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Location After End of Buffer			a memory corruption 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-2021-36015**	ecurity/products/media-encoder/apsb21-43.html	020921/695
Out-of-bounds Read	20-Aug-21	4.3	Adobe Media Encoder version 15.2 (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 read arbitrary file system 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-2021-36016**	https://helpx.adobe.com/security/products/media-encoder/apsb21-43.html	O-MIC-WIND-020921/696
Motorola					
mm1000_firmware					
Improper Authentication	17-Aug-21	2.1	The Motorola MM1000 device configuration portal can be accessed without authentication, which could allow adapter settings to be modified. **CVE ID : CVE-2021-3458**	https://motorolamentor.zendesk.com/hc/en-us/articles/12608040477 50	O-MOT-MM10-020921/697
Improper Neutralization of Special	17-Aug-21	7.2	A privilege escalation vulnerability was reported in the MM1000 device	https://motorolamentor.zendesk.com/	O-MOT-MM10-020921/698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			configuration web server, which could allow privileged shell access and/or arbitrary privileged commands to be executed on the adapter. **CVE ID : CVE-2021-3459**	hc/en-us/articles/12608040477 50	
netmodule					
nb1600_firmware					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	O-NET-NB16-020921/699
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB16-020921/700
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and	https://www.netmodule.com	O-NET-NB16-020921/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**		
nb1601_firmware					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	O-NET-NB16-020921/702
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB16-020921/703
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800,	https://www.netmodule.com	O-NET-NB16-020921/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**		
nb1800_firmware					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	O-NET-NB18-020921/705
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB18-020921/706
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800,	https://www.netmodule.com	O-NET-NB18-020921/707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**		
nb1810_firmware					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	O-NET-NB18-020921/708
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB18-020921/709
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710,	https://www.netmodule.com	O-NET-NB18-020921/710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**		
nb2700_firmware					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	O-NET-NB27-020921/711
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB27-020921/712
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700,	https://www.netmodule.com	O-NET-NB27-020921/713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**		
nb2710_firmware					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	O-NET-NB27-020921/714
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB27-020921/715
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711,	https://www.netmodule.com	O-NET-NB27-020921/716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NB3720, and NB3800. **CVE ID : CVE-2021-39291**		
nb2800_firmware					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	O-NET-NB28-020921/717
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB28-020921/718
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800.	https://www.netmodule.com	O-NET-NB28-020921/719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39291		
nb2810_firmware					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	O-NET-NB28-020921/720
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB28-020921/721
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	O-NET-NB28-020921/722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nb3700_firmware					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	O-NET-NB37-020921/723
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB37-020921/724
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	O-NET-NB37-020921/725
nb3701_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	http://seclists.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	O-NET-NB37-020921/726
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB37-020921/727
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	O-NET-NB37-020921/728
nb3710_firmware					
Insecure	23-Aug-21	5	Certain NetModule devices	http://seclist	O-NET-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Storage of Sensitive Information			have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	s.org/fulldisclosure/2021/Aug/22, https://www.netmodule.com	NB37-020921/729
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB37-020921/730
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	O-NET-NB37-020921/731
nb3711_firmware					
Insecure Storage of	23-Aug-21	5	Certain NetModule devices have Insecure Password	http://seclists.org/fulldisc	O-NET-NB37-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	losure/2021/Aug/22, https://www.netmodule.com	020921/732
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB37-020921/733
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	O-NET-NB37-020921/734
nb3720_firmware					
Insecure Storage of Sensitive	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or	http://seclists.org/fulldisclosure/2021	O-NET-NB37-020921/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	/Aug/22, https://www.netmodule.com	
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB37-020921/736
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	O-NET-NB37-020921/737
nb3800_firmware					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These	http://seclists.org/fulldisclosure/2021/Aug/22,	O-NET-NB38-020921/738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	https://www.netmodule.com	
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB38-020921/739
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	O-NET-NB38-020921/740
nb800_firmware					
Insecure Storage of Sensitive Information	23-Aug-21	5	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before	http://seclists.org/fulldisclosure/2021/Aug/22, https://www	O-NET-NB80-020921/741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39289**	.netmodule.com	
Session Fixation	23-Aug-21	7.5	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39290**	https://www.netmodule.com	O-NET-NB80-020921/742
Incorrect Authorization	23-Aug-21	6.5	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800. **CVE ID : CVE-2021-39291**	https://www.netmodule.com	O-NET-NB80-020921/743
Siemens					
sentron_3wa_com190_firmware					
Improper Input Validation	19-Aug-21	5	An issue was discovered in tcp_rcv() in nptcp.c in HCC embedded InterNiche 4.0.1. The TCP header processing	https://cert-portal.siemens.com/productcert/pdf/s	O-SIE-SENT-020921/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code doesn't sanitize the value of the IP total length field (header length + data length). With a crafted IP packet, an integer overflow occurs whenever the value of the IP data length is calculated by subtracting the length of the header from the total length of the IP packet. **CVE ID : CVE-2021-31401**	sa-789208.pdf	
sentron_3wl_com35_firmware					
Improper Input Validation	19-Aug-21	5	An issue was discovered in tcp_rcv() in nptcp.c in HCC embedded InterNiche 4.0.1. The TCP header processing code doesn't sanitize the value of the IP total length field (header length + data length). With a crafted IP packet, an integer overflow occurs whenever the value of the IP data length is calculated by subtracting the length of the header from the total length of the IP packet. **CVE ID : CVE-2021-31401**	https://cert-portal.siemens.com/productcert/pdf/ssa-789208.pdf	O-SIE-SENT-020921/745
totolink					
a3002r_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-21	4.3	Cross-site scripting in ddns.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "Domain Name" field, "Server Address" field, "User Name/Email", or	N/A	O-TOT-A300-020921/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"Password/Key" field. **CVE ID : CVE-2021-34207**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-21	4.3	Cross-site scripting in tcpipwan.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "Service Name" field. **CVE ID : CVE-2021-34215**	N/A	O-TOT-A300-020921/747
N/A	20-Aug-21	5	Directory Indexing in Login Portal of Login Portal of TOTOLINK-A702R-V1.0.0-B20161227.1023 allows attacker to access /add/ , /img/, /js/, and /mobile directories via GET Parameter. **CVE ID : CVE-2021-34218**	N/A	O-TOT-A300-020921/748
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-21	4.3	Cross-site scripting in tr069config.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "User Name" field or "Password" field. **CVE ID : CVE-2021-34220**	N/A	O-TOT-A300-020921/749
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-21	4.3	Cross-site scripting in urlfilter.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "URL Address" field. **CVE ID : CVE-2021-34223**	N/A	O-TOT-A300-020921/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-21	4.3	Cross-site scripting in parent_control.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "Description" field and "Service Name" field. **CVE ID : CVE-2021-34228**	N/A	O-TOT-A300-020921/751
Tp-link					
tl-wr840n_firmware					
Exposure of Resource to Wrong Sphere	19-Aug-21	4.3	In TP-Link Wireless N Router WR840N an ARP poisoning attack can cause buffer overflow **CVE ID : CVE-2021-29280**	N/A	O-TP--TL-W-020921/752