Vulnerability Summary for the Week of August 16, 2021

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by Ug-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of Ug-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- application_extension_platform	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	2021-08-18	10	CVE-2021-34730 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
dated_news_project -- dated_news	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 allows SQL Injection.	2021-08-13	7.5	CVE-2021-36789 MISC MISC
throughtek -- kalay_p2p_software_development_kit	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.	2021-08-17	7.6	CVE-2021-28372 MISC MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dated_news_project -- dated_news	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 has incorrect Access Control for confirming various applications.	2021-08-13	6.4	CVE-2021-36792 MISC MISC
dated_news_project -- dated_news	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 allows Information Disclosure of application registration data.	2021-08-13	5	CVE-2021-36791 MISC CONFIRM
dated_news_project -- dated_news	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 allows XSS.	2021-08-13	4.3	CVE-2021-36790 MISC MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. In affected versions when running shape functions, some functions (such as `MutableHashTableShape`) produce extra output information in the form of a `ShapeAndType` struct. The shapes embedded in this struct are owned by an inference context that is cleaned up almost	2021-08-13	4.6	CVE-2021-37690 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	immediately; if the upstream code attempts to access this shape information, it can trigger a segfault. `ShapeRefiner` is mitigating this for normal output shapes by cloning them (and thus putting the newly created shape under ownership of an inference context that will not die), but we were not doing the same for shapes and types. This commit fixes that by doing similar logic on output shapes and types. We have patched the issue in GitHub commit ee119d4a498979525046fba1c3dd3f13a039fbb1. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.			
routes_project -- routes	The routes (aka Extbase Yaml Routes) extension before 2.1.1 for TYPO3, when CsrfTokenViewHelper is used, allows Sensitive Information Disclosure because a session identifier is unsafely present in HTML output.	2021-08-13	5	CVE-2021-36793 CONFIRM MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
miniorange -- saml	The miniorange_saml (aka Miniorange Saml) extension before 1.4.3 for TYPO3 allows XSS.	2021-08-13	3.5	CVE-2021-36785 MISC CONFIRM
yoast -- yoast_seo	The yoast_seo (aka Yoast SEO) extension before 7.2.3 for TYPO3 allows XSS.	2021-08-13	3.5	CVE-2021-36788 MISC CONFIRM

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mediatek -- ged	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	2021-08-18	not yet calculated	CVE-2021-0626 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation. Patch ID: ALPS05687510; Issue ID: ALPS05687510.			
abb -- power_grids_retail_operations_and_counterpay_settlement_billing	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.	2021-08-20	not yet calculated	CVE-2021-35529 CONFIRM CONFIRM
adobe -- acrobat_reader_dc	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 Read vulnerability. 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.	2021-08-20	not yet calculated	CVE-2021-35988 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat_reader_dc	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by an Type Confusion vulnerability. An unauthenticated attacker could leverage this vulnerability to read arbitrary 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.	2021-08-20	not yet calculated	CVE-2021-35986 MISC
adobe -- acrobat_reader_dc	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-08-20	not yet calculated	CVE-2021-35985 MISC
adobe -- acrobat_reader_dc	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 Read vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose arbitrary memory information in the context of the	2021-08-20	not yet calculated	CVE-2021-35987 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
adobe -- acrobat_reader_dc	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by a Null pointer dereference vulnerability. An authenticated attacker could leverage this vulnerability achieve an application denial-of-service in the context of the current user. Exploitation of this issue does not requires user interaction.	2021-08-20	not yet calculated	CVE-2021-35984 MISC
adobe -- acrobat_reader_dc	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.	2021-08-20	not yet calculated	CVE-2021-35983 MISC
adobe -- acrobat_reader_dc	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-	2021-08-20	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.		calculated	35981 MISC
adobe -- bridge	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.	2021-08-20	not yet calculated	CVE-2021-35989 MISC
adobe -- bridge	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.	2021-08-20	not yet calculated	CVE-2021-35992 MISC
adobe -- bridge	Adobe Bridge version 11.0.2 (and earlier) are affected by a Heap-based Buffer overflow	2021-08-20	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.		calculated	28624 MISC
adobe -- bridge	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.	2021-08-20	not yet calculated	CVE-2021-35990 MISC
adobe -- bridge	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.	2021-08-20	not yet calculated	CVE-2021-35991 MISC
adobe -- character_animator	Adobe Character Animator version 4.2 (and earlier) is affected by a memory corruption vulnerability	2021-08-20	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.		calculated	36000 MISC
adobe -- character_animator	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 malicious file.	2021-08-20	not yet calculated	CVE-2021-36001 MISC
adobe -- dimension	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.	2021-08-20	not yet calculated	CVE-2021-28595 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- illustrator	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.	2021-08-20	not yet calculated	CVE-2021-28593 MISC
adobe -- illustrator	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.	2021-08-20	not yet calculated	CVE-2021-36011 MISC
adobe -- illustrator	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.	2021-08-20	not yet calculated	CVE-2021-36010 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- illustrator	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.	2021-08-20	not yet calculated	CVE-2021-36009 MISC
adobe -- illustrator	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.	2021-08-20	not yet calculated	CVE-2021-36008 MISC
adobe -- illustrator	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.	2021-08-20	not yet calculated	CVE-2021-28591 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- illustrator	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.	2021-08-20	not yet calculated	CVE-2021-28592 MISC
adobe -- media_encoder	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.	2021-08-20	not yet calculated	CVE-2021-36014 MISC
adobe -- media_encoder	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	2021-08-20	not yet calculated	CVE-2021-36016 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	issue requires user interaction in that a victim must open a malicious file.			
adobe -- media_encoder	Adobe Media Encoder 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.	2021-08-20	not yet calculated	CVE-2021-36015 MISC
adobe -- media_encoer	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.	2021-08-20	not yet calculated	CVE-2021-28589 MISC
adobe -- media_encoer	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	2021-08-20	not yet calculated	CVE-2021-28590 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
adobe -- photoshop	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.	2021-08-20	not yet calculated	CVE-2021-36006 MISC
adobe -- photoshop	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.	2021-08-20	not yet calculated	CVE-2021-36005 MISC
adobe -- prelude	Adobe Prelude version 10.0 (and earlier) is affected by a memory corruption vulnerability when parsing a	2021-08-20	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.		calculated	35999 MISC
adobe -- prelude	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 of this issue requires user interaction in that a victim must open a malicious file.	2021-08-20	not yet calculated	CVE-2021-36007 MISC
adobe -- premiere_pro	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.	2021-08-20	not yet calculated	CVE-2021-35997 MISC
adobe -- reader_dc	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and	2021-08-20	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.		calculated	28642 MISC
adobe -- reader_dc	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.	2021-08-20	not yet calculated	CVE-2021-28641 MISC
adobe -- reader_dc	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by an Uncontrolled Search Path Element vulnerability. An attacker with access to the victim's C:/ folder 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.	2021-08-20	not yet calculated	CVE-2021-28636 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- reader_dc	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.	2021-08-20	not yet calculated	CVE-2021-28643 MISC
adobe -- reader_dc	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by an Improper Neutralization of Special Elements used in an OS Command. An authenticated attacker could leverage this vulnerability to achieve arbitrary code execution on the host machine in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-08-20	not yet calculated	CVE-2021-28634 MISC
adobe -- reader_dc	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by a Heap-based Buffer overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in	2021-08-20	not yet calculated	CVE-2021-28638 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
adobe -- reader_dc	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by a 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.	2021-08-20	not yet calculated	CVE-2021-28635 MISC
adobe -- reader_dc	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 read vulnerability. An unauthenticated attacker could leverage this vulnerability achieve arbitrary read / write 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.	2021-08-20	not yet calculated	CVE-2021-28637 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- reader_dc	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.	2021-08-20	not yet calculated	CVE-2021-28640 MISC
adobe -- reader_dc	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.	2021-08-20	not yet calculated	CVE-2021-28639 MISC
aitecms -- aitecms	SQL Injection in AiteCMS v1.0 allows remote attackers to execute arbitrary code via the component "aitecms/login/diy_list.php".	2021-08-18	not yet calculated	CVE-2020-18746 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ansi-html -- ansi-html	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.	2021-08-18	not yet calculated	CVE-2021-23424 MISC MISC MISC
apache -- airflow	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 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.	2021-08-16	not yet calculated	CVE-2021-35936 MISC
apache -- http/2	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.	2021-08-16	not yet calculated	CVE-2021-33193 MISC MISC
apache -- ofbiz	Unrestricted Upload of File with Dangerous Type vulnerability in Apache OFBiz allows an attacker to execute remote commands. This issue affects Apache	2021-08-18	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.		calculated	37608 MISC
appdynamics -- appdynamics	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.	2021-08-18	not yet calculated	CVE-2021-34745 CONFIRM
at&t -- labs	A heap-based buffer overflow vulnerability exists in the XML Decompression DecodeTreeBlock functionality 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.	2021-08-20	not yet calculated	CVE-2021-21828 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
at&t -- labs	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.	2021-08-17	not yet calculated	CVE-2021-21810 MISC
at&t -- labs	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 lead to remote code execution. An attacker can provide a malicious file to trigger this vulnerability.	2021-08-18	not yet calculated	CVE-2021-21825 MISC
at&t -- labs	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.	2021-08-20	not yet calculated	CVE-2021-21826 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
at&t -- labs	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.	2021-08-20	not yet calculated	CVE-2021-21827 MISC
atlassian -- jira_server_and_data_center	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.	2021-08-16	not yet calculated	CVE-2021-26086 MISC
atutor -- atutor	A reflected cross site scripting (XSS) vulnerability in the /header.tmpl.php component of ATutor 2.2.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	2021-08-17	not yet calculated	CVE-2020-23341 MISC
baserow -- baserow	SSRF in URL file upload in Baserow <1.1.0 allows remote authenticated users to retrieve files from the	2021-08-20	not yet	CVE-2021-22255

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	internal server network exposed over HTTP by inserting an internal address.		calculated	MISC MISC CONFIRM
bblfshd -- bblfshd	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 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.	2021-08-16	not yet calculated	CVE-2021-32825 MISC CONFIRM MISC
bento4 -- bento4	A heap-based buffer overflow exists in the AP4_StdcFileByteStream::ReadPartial component located in /StdC/Ap4StdCFileByteStream.cpp of Bento4 version 06c39d9. This issue can lead to a denial of service (DOS).	2021-08-17	not yet calculated	CVE-2020-23332 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bento4 -- bento4	A heap-based buffer overflow exists in the AP4_CttsAtom::AP4_CttsAtom component located in /Core/Ap4Utils.h of Bento4 version 06c39d9. This can lead to a denial of service (DOS).	2021-08-17	not yet calculated	CVE-2020-23333 MISC
bento4 -- bento4	A WRITE memory access in the AP4_NullTerminatedStringAtom::AP4_NullTerminatedStringAtom component of Bento4 version 06c39d9 can lead to a segmentation fault.	2021-08-17	not yet calculated	CVE-2020-23334 MISC
bento4 -- bento4	An issue was discovered in Bento4 version 06c39d9. A NULL pointer dereference exists in the AP4_Stz2Atom::GetSampleSize component located in /Core/Ap4Stz2Atom.cpp. It allows an attacker to cause a denial of service (DOS).	2021-08-17	not yet calculated	CVE-2020-23330 MISC
bento4 -- bento4	An issue was discovered in Bento4 version 06c39d9. A NULL pointer dereference exists in the AP4_DescriptorListWriter::Action component located in /Core/Ap4Descriptor.h. It allows an attacker to cause a denial of service (DOS).	2021-08-17	not yet calculated	CVE-2020-23331 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bikeshed -- bikeshed	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.	2021-08-16	not yet calculated	CVE-2021-23423 MISC MISC
bikeshed -- bikeshed	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.	2021-08-16	not yet calculated	CVE-2021-23422 CONFIRM CONFIRM
bind -- supported_preview_edition	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.	2021-08-18	not yet calculated	CVE-2021-25218 CONFIRM MLIST MLIST FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
blackberry -- qnx_software_development_platform	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.	2021-08-17	not yet calculated	CVE-2021-22156 MISC CISCO
bludit -- bluedit	Unrestricted File Upload in Bludit v3.8.1 allows remote attackers to execute arbitrary code by uploading malicious files via the component 'bl-kereln/ajax/upload-logo.php'.	2021-08-20	not yet calculated	CVE-2020-18879 MISC
bssa -- dft	Insecure default variable initialization for the Intel BSSA DFT feature may allow a privileged user to potentially enable an escalation of privilege via local access.	2021-08-16	not yet calculated	CVE-2021-0114 MISC
centreon -- centreon	/graphStatus/displayServiceStatus.php in Centreon 19.10.8 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the RRDdatabase_path parameter.	2021-08-18	not yet calculated	CVE-2020-22345 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- expressway_series	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.	2021-08-18	not yet calculated	CVE-2021-34715 CISCO
cisco -- expressway_series	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	2021-08-18	not yet calculated	CVE-2021-34716 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.			
cisco -- secure_email_and_web_manager	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.	2021-08-18	not yet calculated	CVE-2021-1561 CISCO
cisco -- video_surveillance_7000_series_ip_cameras	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,	2021-08-18	not yet calculated	CVE-2021-34734 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	referred to 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).			
cisco -- web_security_appliance	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 perform additional data exfiltration attacks.	2021-08-18	not yet calculated	CVE-2021-34749 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
citrix -- sharefile	An issue has been identified in the CTX269106 mitigation tool for Citrix ShareFile storage zones controller which causes the ShareFile file encryption option to become disabled if it had previously been enabled. Customers are only affected by this issue if they previously selected “Enable Encryption” in the ShareFile configuration page and did not re-select this setting after running the CTX269106 mitigation tool. ShareFile customers who have not run the CTX269106 mitigation tool or who re-selected “Enable Encryption” immediately after running the tool are unaffected by this issue.	2021-08-16	not yet calculated	CVE-2021-22932 MISC
clickhouse -- clickhouse	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.	2021-08-17	not yet calculated	CVE-2021-25263 MISC
codesys -- gmbh	A unsafe deserialization vulnerability exists in the ObjectManager.plugin Project.get_MissingTypes() 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.	2021-08-18	not yet calculated	CVE-2021-21868 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codesys -- gmbh	A 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.	2021-08-18	not yet calculated	CVE-2021-21867 MISC
crocoblock -- jetengine	Crocoblock JetEngine before 2.6.1 allows XSS by remote authenticated users via a custom form input.	2021-08-16	not yet calculated	CVE-2021-38607 CONFIRM MISC
cyberoam -- netgenie	Cyberoam NetGenie C0101B1-20141120-NG11VO devices through 2021-08-14 allow tweb/ft.php?u=[XSS] attacks.	2021-08-17	not yet calculated	CVE-2021-38702 MISC MISC MISC FULLDISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20771 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20758 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20766 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20768 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cybozu -- garoon	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 privilege.	2021-08-18	not yet calculated	CVE-2021-20755 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20756 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20759 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20753 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20754 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20757 MISC MISC
cybozu -- garoon	Improper input validation vulnerability in User Profile of 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.	2021-08-18	not yet calculated	CVE-2021-20760 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20775 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20762 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20761 MISC MISC
cybozu -- garoon	Cross-site scripting vulnerability in some functions of E-mail of Cybozu Garoon 4.0.0 to 5.5.0 allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	2021-08-18	not yet calculated	CVE-2021-20774 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20763 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20767 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20770 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20769 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20764 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20772 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20773 MISC MISC
cybozu -- garoon	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.	2021-08-18	not yet calculated	CVE-2021-20765 MISC MISC
d-link -- dsl-2750u_router	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.	2021-08-16	not yet calculated	CVE-2021-3707 MISC JVN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
d-link -- dsl-2750u_router	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.	2021-08-16	not yet calculated	CVE-2021-3708 MISC JVN CONFIRM
dell -- emc_powerscale_onefs	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.	2021-08-16	not yet calculated	CVE-2021-21594 CONFIRM
dell -- emc_powerscale_onefs	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.	2021-08-16	not yet calculated	CVE-2021-36280 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- emc_powerscale_onefs	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.	2021-08-16	not yet calculated	CVE-2021-36279 CONFIRM
dell -- emc_powerscale_onefs	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.	2021-08-16	not yet calculated	CVE-2021-36281 CONFIRM
dell -- emc_powerscale_onefs	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.	2021-08-16	not yet calculated	CVE-2021-21592 CONFIRM
dell -- emc_powerscale_onefs	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	2021-08-16	not yet calculated	CVE-2021-21599 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	impacts Smartlock WORM compliance mode clusters as a critical vulnerability and Dell recommends to update/upgrade at the earliest opportunity.			
dell -- emc_powerscale_onefs	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.x contain an insufficient logging 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.	2021-08-16	not yet calculated	CVE-2021-21568 CONFIRM
dell -- emc_powerscale_onefs	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.	2021-08-16	not yet calculated	CVE-2021-36282 CONFIRM
dell -- emc_powerscale_onefs	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	2021-08-16	not yet calculated	CVE-2021-36278 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ISI_PRIV_LOGIN_CONSOLE privileges can access privileged information.			
dell -- emc_powerscale_onefs	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 update/upgrade at the earliest opportunity.	2021-08-16	not yet calculated	CVE-2021-21595 CONFIRM
diez -- diez	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.	2021-08-17	not yet calculated	CVE-2021-32830 CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
disc_soft_ltd -- deamon_tools_pro	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.	2021-08-17	not yet calculated	CVE-2021-21832 MISC
django-widgy -- django-widgy	Unrestricted Upload of File with Dangerous Type in Django-Widgy v0.8.4 allows remote attackers to execute arbitrary code via the 'image' widget in the component 'Change Widgy Page'.	2021-08-16	not yet calculated	CVE-2020-18704 MISC
dolibarr -- dolibarr	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.	2021-08-17	not yet calculated	CVE-2021-25956 MISC MISC
dolibarr -- dolibarr	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	2021-08-17	not yet calculated	CVE-2021-25957

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	password reset link the user received through email when requested for a forgotten password.			MISC MISC
dolibarr -- dolibarr	In “Dolibarr ERP CRM”, WYSIWYG Editor module, v2.8.1 to v13.0.2 are affected by a stored XSS vulnerability that allows low privileged application users to store malicious scripts in the “Private Note” field at “/adherents/note.php?id=1” endpoint. These scripts are executed in a victim’s browser when they open the page containing the vulnerable field. In the worst case, the victim who inadvertently triggers the attack is a highly privileged administrator. The injected scripts can extract the Session ID, which can lead to full Account takeover of the admin and due to other vulnerability (Improper Access Control on Private notes) a low privileged user can update the private notes which could lead to privilege escalation.	2021-08-15	not yet calculated	CVE-2021-25955 MISC MISC
dotcms -- dotcms	Incorrect Access Control in DotCMS versions before 5.1 allows remote attackers to gain privileges by injecting client configurations via vtl (velocity) files.	2021-08-18	not yet calculated	CVE-2020-18875 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eclipse -- californium	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.	2021-08-20	not yet calculated	CVE-2021-34433 CONFIRM
empirecms -- empirecms	A remote code execution (RCE) in e/install/index.php of EmpireCMS 7.5 allows attackers to execute arbitrary PHP code via writing malicious code to the install file.	2021-08-17	not yet calculated	CVE-2020-22937 MISC
evoucms -- evoucms	Cross Site Request Forgery (CSRF) vulnerability exists in EyouCMS 1.3.6 that can add an htm page to execute the js code via login.php?m=admin&c=Filemanager&a=newfile&lang=cn.	2021-08-19	not yet calculated	CVE-2020-20642 MISC
evoucms -- evoucms	Cross Site Scripting (XSS) vulnerability exists in Eyoucms v1.4.7 and earlier via the addonfieldext parameter.	2021-08-18	not yet calculated	CVE-2020-28146 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
evoucms -- evoucms	Cross Site Request Forgery (CSRF) vulnerability exists in Eyoucms 1.3.6 that can add an admin account via /login.php?m=admin&c=Admin&a=admin_add&lang=cn.	2021-08-18	not yet calculated	CVE-2020-19669 MISC
exiv2 -- exiv2	An uncontrolled memory allocation in DataBufdata(subBox.length-sizeof(box)) function of Exiv2 0.27 allows attackers to cause a denial of service (DOS) via a crafted input.	2021-08-19	not yet calculated	CVE-2020-18899 MISC
exiv2 -- exiv2	A stack exhaustion issue in the printIFDStructure function of Exiv2 0.27 allows remote attackers to cause a denial of service (DOS) via a crafted file.	2021-08-19	not yet calculated	CVE-2020-18898 MISC
exponentcms -- exponentcms	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.	2021-08-16	not yet calculated	CVE-2021-38751 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eyoucms -- eyoucms	Cross Site Scripting (XSS) vulnerability exists in EyouCMS1.3.6 in the basic_information area.	2021-08-19	not yet calculated	CVE-2020-20645 MISC
ffmpeg -- ffmpeg	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.	2021-08-21	not yet calculated	CVE-2021-38171 MISC MISC
fortinet -- fortiportal	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 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.	2021-08-19	not yet calculated	CVE-2021-32602 CONFIRM
fortinet -- fortiportal	A use of hard-coded credentials (CWE-798) vulnerability in FortiPortal versions 5.2.5 and below,	2021-08-18	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.		calculated	32588 CONFIRM
gitit -- gitit	In gitit before 0.15.0.0, the Export feature can be exploited to leak information from files.	2021-08-16	not yet calculated	CVE-2021-38711 MISC MISC
gitlab -- ce/ee	Under very specific conditions a user could be impersonated using Gitlab shell. This vulnerability affects GitLab CE/EE 13.1 and later through 14.1.2, 14.0.7 and 13.12.9.	2021-08-20	not yet calculated	CVE-2021-22254 MISC MISC CONFIRM
gitlab -- gitlab	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.	2021-08-20	not yet	CVE-2021-22238

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
			calculated	MISC MISC CONFIRM
gitlab -- webhook	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.	2021-08-20	not yet calculated	CVE-2021-22246 MISC MISC CONFIRM
gmbh -- komoot	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.	2021-08-20	not yet calculated	CVE-2021-21823 MISC
google -- android	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:	2021-08-17	not yet calculated	CVE-2021-0579 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	AndroidVersions: Android SoCAndroid ID: A-187231636			
google -- android	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	2021-08-17	not yet calculated	CVE-2021-0584 MISC
google -- android	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	2021-08-17	not yet calculated	CVE-2021-0646 MISC
google -- android	In shouldBlockFromTree of ExternalStorageProvider.java, there is a possible	2021-08-17	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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		calculated	0645 MISC
google -- android	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-187161772	2021-08-17	not yet calculated	CVE-2021-0578 MISC
google -- android	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	2021-08-17	not yet calculated	CVE-2021-0574 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	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	2021-08-17	not yet calculated	CVE-2021-0576 MISC
google -- android	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	2021-08-17	not yet calculated	CVE-2021-0642 MISC
google -- android	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	2021-08-17	not yet calculated	CVE-2021-0641 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Android-9 Android-10 Android-11Android ID: A-185235454			
google -- android	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 additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-187957589	2021-08-17	not yet calculated	CVE-2021-0640 MISC
google -- android	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	2021-08-17	not yet calculated	CVE-2021-0639 MISC
google -- android	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	2021-08-17	not yet calculated	CVE-2021-0580 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187231637			
google -- android	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-187231638	2021-08-17	not yet calculated	CVE-2021-0581 MISC
google -- android	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-187231635	2021-08-17	not yet calculated	CVE-2021-0573 MISC
google -- android	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	2021-08-17	not yet calculated	CVE-2021-0519 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-176533109			
google -- android	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	2021-08-17	not yet calculated	CVE-2021-0593 MISC
google -- android	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 needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-179386960	2021-08-17	not yet calculated	CVE-2021-0591 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	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	2021-08-17	not yet calculated	CVE-2021-0582 MISC
google -- google	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)`.	2021-08-17	not yet calculated	CVE-2021-39131 MISC CONFIRM MISC
gpac_project -- advanced_content_library	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.	2021-08-18	not yet calculated	CVE-2021-21856 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac_project -- advanced_content_library	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 “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.	2021-08-18	not yet calculated	CVE-2021-21852 MISC MISC
gpac_project -- advanced_content_library	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.	2021-08-18	not yet calculated	CVE-2021-21855 MISC
gpac_project -- advanced_content_library	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	2021-08-18	not yet calculated	CVE-2021-21846 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
gpac_project -- advanced_content_library	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.	2021-08-18	not yet calculated	CVE-2021-21837 MISC MISC
gpac_project -- advanced_content_library	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.	2021-08-16	not yet calculated	CVE-2021-21859 MISC
gpac_project -- advanced_content_library	Multiple exploitable integer overflow vulnerabilities exist within the MPEG-4 decoding functionality of	2021-08-18	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.		calculated	21844 MISC MISC
gpac_project -- advanced_content_library	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.	2021-08-16	not yet calculated	CVE-2021-21861 MISC
gpac_project -- advanced_content_library	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	2021-08-18	not yet calculated	CVE-2021-21858 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	that causes memory corruption. An attacker can convince a user to open a video to trigger this vulnerability.			
gpac_project -- advanced_content_library	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.	2021-08-18	not yet calculated	CVE-2021-21854 MISC
gpac_project -- advanced_content_library	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.	2021-08-18	not yet calculated	CVE-2021-21847 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac_project -- advanced_content_library	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.	2021-08-16	not yet calculated	CVE-2021-21860 MISC
gpac_project -- advanced_content_library	Multiple exploitable integer truncation 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 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.	2021-08-18	not yet calculated	CVE-2021-21862 MISC
gpac_project -- advanced_content_library	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	2021-08-18	not yet calculated	CVE-2021-21851 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
gpac_project -- advanced_content_library	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.	2021-08-18	not yet calculated	CVE-2021-21838 MISC MISC
gpac_project -- advanced_content_library	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.	2021-08-18	not yet calculated	CVE-2021-21857 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac_project -- advanced_content_library	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 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.	2021-08-18	not yet calculated	CVE-2021-21843 MISC MISC
gpac_project -- advanced_content_library	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.	2021-08-18	not yet calculated	CVE-2021-21853 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac_project -- advanced_content_library	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.	2021-08-18	not yet calculated	CVE-2021-21839 MISC MISC
gpac_project -- advanced_content_library	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 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.	2021-08-18	not yet calculated	CVE-2021-21845 MISC MISC
handlebars -- handlebars	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	2021-08-16	not yet calculated	CVE-2021-32822 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
haproxy -- haproxy	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.	2021-08-17	not yet calculated	CVE-2021-39242 MISC MISC DEBIAN
haproxy -- haproxy	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.	2021-08-17	not yet calculated	CVE-2021-39241 MISC MISC DEBIAN
haproxy -- haproxy	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	2021-08-17	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.		calculated	39240 MISC MISC MISC DEBIAN
hospital_management_system -- hospital_management_system	Persistent cross-site scripting (XSS) in Hospital Management System targeted towards web admin through contact.php.	2021-08-16	not yet calculated	CVE-2021-38757 MISC MISC
hospital_management_system -- hospital_management_system	Unauthenticated doctor entry deletion in Hospital Management System in admin-panel1.php.	2021-08-16	not yet calculated	CVE-2021-38755 MISC
hospital_management_system -- hospital_management_system	SQL Injection vulnerability in Hospital Management System due to lack of input validation in messearch.php.	2021-08-16	not yet calculated	CVE-2021-38754 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hospital_management_system -- hospital_management_system	Persistent cross-site scripting (XSS) in Hospital Management System targeted towards web admin through prescribe.php.	2021-08-16	not yet calculated	CVE-2021-38756 MISC
ibm -- api_connect	IBM API Connect 5.0.0.0 through 5.0.8.10 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. By sending a specially crafted HTTP request, a remote attacker could exploit this vulnerability to inject HTTP HOST header, which will allow the attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 187194.	2021-08-17	not yet calculated	CVE-2020-4706 CONFIRM XF
ibm -- datapower_gateway	IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.16 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 192737.	2021-08-17	not yet calculated	CVE-2020-4992 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
icinga -- multiple_product	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.	2021-08-19	not yet calculated	CVE-2021-37698 MISC CONFIRM MISC MISC
imcat -- imcat	A remote code execution (RCE) vulnerability in /root/run/adm.php?admin-ediy&part=exdiy of imcat v5.1 allows authenticated attackers to execute arbitrary code.	2021-08-18	not yet calculated	CVE-2020-22120 MISC
imgurl -- imgurl	imgURL 2.31 allows XSS via an X-Forwarded-For HTTP header.	2021-08-16	not yet calculated	CVE-2021-38713 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
interniche -- nichestack	The DNS feature in InterNiche NicheStack TCP/IP 4.0.1 is affected by: Out-of-bounds Read. The impact is: a denial of service (remote). The component is: DNS response processing in function: dns_upcall(). The attack vector is: a specific DNS response packet. The code does not check whether the number of queries/responses specified in the DNS packet header corresponds to the query/response data available in the DNS packet.	2021-08-18	not yet calculated	CVE-2020-25927 CERT-VN MISC MISC
interniche -- nichestack	An issue was discovered in HCC Nichestack 3.0. The code that parses TCP packets relies on an unchecked value of the IP payload size (extracted from the IP header) to compute the length of the TCP payload within the TCP checksum computation function. When the IP payload size is set to be smaller than the size of the IP header, the TCP checksum computation function may read out of bounds (a low-impact write-out-of-bounds is also possible).	2021-08-19	not yet calculated	CVE-2020-35684 CONFIRM MISC CERT-VN MISC
interniche -- nichestack	The DNS feature in InterNiche NicheStack TCP/IP 4.0.1 is affected by: Buffer Overflow. The impact is: execute arbitrary code (remote). The component is: DNS response processing functions: dns_upcall(), getoffset(), dnc_set_answer(). The attack vector is: a	2021-08-18	not yet calculated	CVE-2020-25928 CERT

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	specific DNS response packet. The code does not check the "response data length" field of individual DNS answers, which may cause out-of-bounds read/write operations, leading to Information leak, Denial-or-Service, or Remote Code Execution, depending on the context.			-VN MISC
interniche -- nichestack	An issue was discovered in HCC Nichestack 3.0. The code that generates Initial Sequence Numbers (ISNs) for TCP connections derives the ISN from an insufficiently random source. As a result, an attacker may be able to determine the ISN of current and future TCP connections and either hijack existing ones or spoof future ones. (Proper ISN generation should aim to follow at least the specifications outlined in RFC 6528.)	2021-08-19	not yet calculated	CVE-2020-35685 CONFIRM MISC CERT -VN MISC
interniche -- nichestack	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).	2021-08-19	not yet calculated	CVE-2021-36762 CERT -VN MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
interniche -- nichestack	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.	2021-08-19	not yet calculated	CVE-2021-27565 MISC CERT-VN MISC MISC
interniche -- nichestack	An issue was discovered in HCC Embedded NicheStack IPv4 4.1. The dnc_copy_in routine for parsing DNS domain names does not check whether a domain name compression pointer is pointing within the bounds of the packet (e.g., forward compression pointer jumps are allowed), which leads to an Out-of-bounds Read, and a Denial-of-Service as a consequence.	2021-08-18	not yet calculated	CVE-2020-25767 CERT-VN MISC
interniche -- nichestack	An issue was discovered in HCC Nichestack 3.0. The code that parses ICMP packets relies on an unchecked value of the IP payload size (extracted from the IP header) to compute the ICMP checksum. When the IP payload size is set to be smaller than the size of the IP header, the ICMP checksum	2021-08-19	not yet calculated	CVE-2020-35683 CONFIRM MISC CERT

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	computation function may read out of bounds, causing a Denial-of-Service.			-VN MISC
interniche -- nichestack	The DNS client in InterNiche NicheStack TCP/IP 4.0.1 is affected by: Insufficient entropy in the DNS transaction id. The impact is: DNS cache poisoning (remote). The component is: dns_query_type(). The attack vector is: a specific DNS response packet.	2021-08-18	not yet calculated	CVE-2020-25926 CERT-VN MISC
invision -- community	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.	2021-08-17	not yet calculated	CVE-2021-39249 MISC MISC
invision -- community	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	2021-08-17	not yet calculated	CVE-2021-39250 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	header, and the ability of an admin to use the templating engine (e.g., Edit HTML).			
joyplus-cms -- joyplus-cms	A vulnerability in the \inc\config.php component of joyplus-cms v1.6 allows attackers to access sensitive information.	2021-08-18	not yet calculated	CVE-2020-22124 MISC
jsoup -- jsoup	jsoup is a Java library for working with HTML. Those using jsoup versions prior to 1.14.2 to parse untrusted 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.	2021-08-18	not yet calculated	CVE-2021-37714 MISC MISC CONFIRM MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	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) 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.	2021-08-17	not yet calculated	CVE-2021-0284 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lenovo -- driver_management	A DLL preloading vulnerability was reported in Lenovo Driver Management prior to version 2.9.0719.1104 that could allow privilege escalation.	2021-08-17	not yet calculated	CVE-2021-3633 MISC
lenovo -- smart_camera	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.	2021-08-17	not yet calculated	CVE-2021-3617 MISC MISC
lenovo -- smart_camera	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.	2021-08-17	not yet calculated	CVE-2021-3616 MISC MISC
lenovo -- smart_camera	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.	2021-08-17	not yet calculated	CVE-2021-3615 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
libpff -- libpff	A heap-based buffer overflow in the libexe_io_handle_read_coff_optional_header function of libyal libexe before 20181128 allows attackers to execute arbitrary code.	2021-08-19	not yet calculated	CVE-2020-18900 MISC
libpff -- libpff	An use-after-free vulnerability in the libpff_item_tree_create_node function of libyal Libpff before 20180623 allows attackers to cause a denial of service (DOS) or execute arbitrary code via a crafted pff file.	2021-08-19	not yet calculated	CVE-2020-18897 MISC MISC
lin-cms-flask -- lin-cms-flask	Incorrect Access Control in Lin-CMS-Flask v0.1.1 allows remote attackers to obtain sensitive information and/or gain privileges due to the application not invalidating a user's authentication token upon logout, which allows for replaying packets.	2021-08-16	not yet calculated	CVE-2020-18701 MISC
lin-cms-flask -- lin-cms-flask	Cross Site Scripting (XSS) in Lin-CMS-Flask v0.1.1 allows remote attackers to execute arbitrary code by entering scripts in the the 'Username' parameter of the in component 'app/api/cms/user.py'.	2021-08-16	not yet calculated	CVE-2020-18699 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lin-cms-flask -- lin-cms-flask	Improper Authentication in Lin-CMS-Flask v0.1.1 allows remote attackers to launch brute force login attempts without restriction via the 'login' function in the component 'app/api/cms/user.py'.	2021-08-16	not yet calculated	CVE-2020-18698 MISC
linux -- linux_kernel	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	2021-08-18	not yet calculated	CVE-2021-21781 MISC
live555 -- live555	liveMedia/FramedSource.cpp in Live555 through 1.08 allows an assertion failure and application exit via multiple SETUP and PLAY commands.	2021-08-18	not yet calculated	CVE-2021-39283 MISC MISC
live555 -- live555	Live555 through 1.08 has a memory leak in AC3AudioStreamParser for AC3 files.	2021-08-18	not yet	CVE-2021-39282

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
			calculated	MISC MISC
ljcms -- ljcms	A SQL injection vulnerability in /oa.php?c=Staff&a=read of Find a Place LJCMS v 1.3 allows attackers to access sensitive database information via a crafted POST request.	2021-08-18	not yet calculated	CVE-2020-22122 MISC
mediatek -- clk_driver	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.	2021-08-18	not yet calculated	CVE-2021-0408 MISC
mediatek -- clk_driver	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.	2021-08-18	not yet calculated	CVE-2021-0407 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mediatek -- memory_management_drier	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: ALPS05336700.	2021-08-18	not yet calculated	CVE-2021-0416 MISC
mediatek -- memory_management_driver	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.	2021-08-18	not yet calculated	CVE-2021-0418 MISC
mediatek -- memory_management_driver	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.	2021-08-18	not yet calculated	CVE-2021-0417 MISC
mediatek -- memory_management_driver	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	2021-08-18	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381065.		calculated	0420 MISC
mediatek -- memory_management_driver	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.	2021-08-18	not yet calculated	CVE-2021-0415 MISC
mediatek -- memory_management_driver	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: ALPS05336713.	2021-08-18	not yet calculated	CVE-2021-0419 MISC
mediatek -- oma_drm	In OMA DRM, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05722434; Issue ID: ALPS05722434.	2021-08-18	not yet calculated	CVE-2021-0627 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mediatek -- oma_drm	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.	2021-08-18	not yet calculated	CVE-2021-0628 MISC
misp -- misp	MISP 2.4.148, in certain configurations, allows SQL injection via the app/Model/Log.php $conditions['org'] value.	2021-08-19	not yet calculated	CVE-2021-39302 MISC
mockserver -- mockserver	MockServer is open source software which enables easy 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	2021-08-16	not yet calculated	CVE-2021-32827 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
motorola -- mm1000	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.	2021-08-17	not yet calculated	CVE-2021-3459 MISC
motorola -- mm1000	The Motorola MM1000 device configuration portal can be accessed without authentication, which could allow adapter settings to be modified.	2021-08-17	not yet calculated	CVE-2021-3458 MISC
mozilla -- firefox	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.	2021-08-17	not yet calculated	CVE-2021-29990 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- firefox	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.	2021-08-17	not yet calculated	CVE-2021-29983 MISC MISC
mozilla -- firefox_and_thunderbird	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.	2021-08-17	not yet calculated	CVE-2021-29984 MISC MISC MISC MISC MISC
mozilla -- firefox_and_thunderbird	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.	2021-08-17	not yet calculated	CVE-2021-29982 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- firefox_and_thunderbird	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.	2021-08-17	not yet calculated	CVE-2021-29986 MISC MISC MISC MISC MISC
mozilla -- firefox_and_thunderbird	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.	2021-08-17	not yet calculated	CVE-2021-29988 MISC MISC MISC MISC MISC
mozilla -- firefox_and_thunderbird	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.	2021-08-17	not yet calculated	CVE-2021-29985 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
mozilla -- firefox_and_thunderbird	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.	2021-08-17	not yet calculated	CVE-2021-29989 MISC MISC MISC MISC
mozilla -- firefox_and_thunderbird	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.	2021-08-17	not yet calculated	CVE-2021-29981 MISC MISC MISC
mozilla -- firefox_and_thunderbird	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.	2021-08-17	not yet calculated	CVE-2021-29980 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
mozilla -- firefox_and_thunderbird	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.	2021-08-17	not yet calculated	CVE-2021-29987 MISC MISC MISC
netsarang -- xshell_7	NetSarang Xshell 7 before Build 0077 includes unintended code strings in paste operations.	2021-08-15	not yet calculated	CVE-2021-37326 MISC
nextcloud -- desktop_client	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	2021-08-18	not yet calculated	CVE-2021-37617 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`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` file on the system.			CONFIRM
nextcloud -- desktop_client	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.	2021-08-18	not yet calculated	CVE-2021-32728 CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nichestack -- interniche	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.	2021-08-19	not yet calculated	CVE-2021-31227 MISC MISC
nichestack -- interniche	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 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.	2021-08-19	not yet calculated	CVE-2021-31226 CERT-VN MISC
nichestack -- interniche	An issue was discovered in HCC embedded InterNiche 4.0.1. This vulnerability allows the attacker to predict a DNS 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	2021-08-19	not yet calculated	CVE-2021-31228 CERT-VN MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	predictable because it is based on the time of day, and has too few bits.			
nichestack -- interniche	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.	2021-08-19	not yet calculated	CVE-2021-31401 CONFIRM CERT-VN MISC
nichestack -- interniche	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).	2021-08-19	not yet calculated	CVE-2021-31400 CERT-VN MISC
node.js -- node.js	Node.js before 16.6.0, 14.17.4, and 12.22.4 is vulnerable to Remote Code Execution, XSS,	2021-08-16	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.		calculated	22931 MISC MISC
node.js -- node.js	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.	2021-08-16	not yet calculated	CVE-2021-22939 MISC MISC
node.js -- node.js	Node.js before 16.6.1, 14.17.5, and 12.22.5 is vulnerable to a use after free attack where an attacker might be able to exploit the memory corruption, to change process behavior.	2021-08-16	not yet calculated	CVE-2021-22940 MISC MISC
ocproducts -- composer	In ocProducts Composr CMS before 10.0.38, an attacker can inject JavaScript via Comcode for XSS.	2021-08-16	not yet calculated	CVE-2021-38708 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ocproducts -- composer	In ocProducts Composr CMS before 10.0.38, an attacker can inject JavaScript via the staff_messaging messaging system for XSS.	2021-08-16	not yet calculated	CVE-2021-38709 MISC
octopus -- server	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.	2021-08-18	not yet calculated	CVE-2021-31820 MISC
oculus -- desktop	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.	2021-08-19	not yet calculated	CVE-2021-24038 CONFIRM
onenav -- onenav	OneNav 0.9.12 allows Information Disclosure of the onenav.db3 contents. NOTE: the vendor's recommended solution is to block the access via an NGINX configuration file.	2021-08-16	not yet calculated	CVE-2021-38712 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
online_catering_reservation_system -- online_catering_reservation_system	Directory traversal in Online Catering Reservation System due to lack of validation in index.php.	2021-08-16	not yet calculated	CVE-2021-38758 MISC
open_edx -- open_edx	Open edX through Lilac.1 allows XSS in common/static/common/js/discussion/utils.js via crafted LaTeX content within a discussion.	2021-08-17	not yet calculated	CVE-2021-39248 MISC
owasp -- csrfguard	In OWASP CSRFGuard through 3.1.0, CSRF can occur because the CSRF cookie may be retrieved by using only a session token.	2021-08-19	not yet calculated	CVE-2021-28490 MISC MISC
parse_server -- parse_server	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Developers can use the REST API to signup users and also allow users to login anonymously. Prior to version 4.5.1, when an anonymous user is first signed up using REST, the server creates session incorrectly. Particularly, the `authProvider` field in `_Session` class under `createdWith` shows the user logged in	2021-08-19	not yet calculated	CVE-2021-39138 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	creating a password. If a developer later depends on the `createdWith` field to provide a different level of access between a password user and anonymous user, the server incorrectly classified the session type as being created with a `password`. The server does not currently use `createdWith` to make decisions about internal functions, so if a developer is not using `createdWith` directly, they are not affected. The vulnerability only affects users who depend on `createdWith` by using it directly. The issue is patched in Parse Server version 4.5.1. As a workaround, do not use the `createdWith` Session field to make decisions if one allows anonymous login.			
phpmywind -- phpmywind	Command Injection in PHPMyWind v5.6 allows remote attackers to execute arbitrary code via the "text color" field of the component '/admin/web_config.php'.	2021-08-20	not yet calculated	CVE-2020-18885 MISC
phpmywind -- phpmywind	Unrestricted File Upload in PHPMyWind v5.6 allows remote attackers to execute arbitrary code via the component 'admin/upload_file_do.php'.	2021-08-20	not yet calculated	CVE-2020-18886 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pimcore -- pimcore	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.	2021-08-18	not yet calculated	CVE-2021-37702 CONFIRM MISC
pixelimity -- pixelimity	Cross Site Scripting (XSS) vulnerability exists in Pixelimity 1.0 via the HTTP POST parameter to admin/setting.php.	2021-08-17	not yet calculated	CVE-2021-29056 MISC
platform -- platform	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.	2021-08-16	not yet calculated	CVE-2021-37711 CONFIRM MISC
ponzu -- ponzu	A cross site request forgery (CSRF) vulnerability in the configure.html component of Ponzu 0.11.0 allows attackers to change user and administrator credentials, and add or delete administrator accounts.	2021-08-20	not yet calculated	CVE-2020-24130 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
prestahome -- blog	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.	2021-08-20	not yet calculated	CVE-2021-36748 MISC MISC MISC
proxyee-down -- proxyee-down	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.	2021-08-16	not yet calculated	CVE-2021-32826 CONFIRM
prussa_research -- prusaslicer	A use-after-free vulnerability exists in the _3MF_Importer::_handle_end_model() functionality of Prusa Research PrusaSlicer 2.2.0 and Master (commit 4b040b856). A specially crafted 3MF file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	2021-08-17	not yet calculated	CVE-2020-28594 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pulse -- connect_secure	A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform command injection via an unsanitized web parameter.	2021-08-16	not yet calculated	CVE-2021-22935 MISC
pulse -- connect_secure	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.	2021-08-16	not yet calculated	CVE-2021-22936 MISC
pulse -- connect_secure	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.	2021-08-16	not yet calculated	CVE-2021-22937 MISC
pulse -- connect_secure	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.	2021-08-16	not yet calculated	CVE-2021-22934 MISC
pulse -- connect_secure	A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to	2021-08-16	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	perform command injection via an unsanitized web parameter in the administrator web console.		calculated	22938 MISC
pulse -- connect_secure	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.	2021-08-16	not yet calculated	CVE-2021-22933 MISC
quiz_and_survey_master -- quiz_and_survey_master	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.	2021-08-18	not yet calculated	CVE-2021-20792 MISC MISC MISC MISC
quokka -- quokka	Cross Site Scripting (XSS) in Quokka v0.4.0 allows remote attackers to execute arbitrary code via the 'Username' parameter in the component 'quokka/admin/actions.py'.	2021-08-16	not yet calculated	CVE-2020-18702 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
quokka -- quokka	XML External Entities (XXE) in Quokka v0.4.0 allows remote attackers to execute arbitrary code via the component 'quokka/core/content/views.py'.	2021-08-16	not yet calculated	CVE-2020-18705 MISC
quokka -- quokka	XML External Entities (XXE) in Quokka v0.4.0 allows remote attackers to execute arbitrary code via the component 'quokka/utils/atom.py'.	2021-08-16	not yet calculated	CVE-2020-18703 MISC
rapid7 -- nexpose	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.	2021-08-19	not yet calculated	CVE-2021-31868 CONFIRM
rconfig -- rconfig	A server-side request forgery (SSRF) vulnerability in rConfig 3.9.5 has been fixed for 3.9.6. This vulnerability allowed remote authenticated attackers to open a connection to the machine via the deviceIpAddr and connPort parameters.	2021-08-20	not yet calculated	CVE-2020-25353 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rconfig -- rconfig	An arbitrary file write vulnerability in lib/AjaxHandlers/ajaxEditTemplate.php of rConfig 3.9.6 allows attackers to execute arbitrary code via a crafted file.	2021-08-20	not yet calculated	CVE-2020-27466 MISC
rconfig -- rconfig	A stored cross-site scripting (XSS) vulnerability in the /devices.php function inrConfig 3.9.5 has been fixed for version 3.9.6. This vulnerability allowed remote attackers to perform arbitrary Javascript execution through entering a crafted payload into the 'Model' field then saving.	2021-08-20	not yet calculated	CVE-2020-25352 MISC
rconfig -- rconfig	An information disclosure vulnerability in rConfig 3.9.5 has been fixed for version 3.9.6. This vulnerability allowed remote authenticated attackers to read files on the system via a crafted request sent to to the /lib/crud/configcompare.crud.php script.	2021-08-20	not yet calculated	CVE-2020-25351 MISC
rconfig -- rconfig	An arbitrary file deletion vulnerability in rConfig 3.9.5 has been fixed for 3.9.6. This vulnerability gave attackers the ability to send a crafted request to /lib/ajaxHandlers/ajaxDeleteAllLoggingFiles.php by specifying a path in the path parameter and an	2021-08-20	not yet calculated	CVE-2020-25359 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	extension in the ext parameter and delete all the files with that extension in that path.			
rconfig -- rconfig	An insecure update feature in the /updater.php component of rConfig 3.9.6 and below allows attackers to execute arbitrary code via a crafted ZIP file.	2021-08-20	not yet calculated	CVE-2020-27464 MISC
realtek -- jungle_sdk	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 an arbitrary command injection vulnerability that can be exploited by remote unauthenticated attackers.	2021-08-16	not yet calculated	CVE-2021-35394 MISC MISC MISC MISC
realtek -- jungle_sdk	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 heap buffer overflow that is present due to unsafe crafting of SSDP NOTIFY messages from received M-SEARCH messages ST header.	2021-08-16	not yet calculated	CVE-2021-35392 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
realtek -- jungle_sdk	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.	2021-08-16	not yet calculated	CVE-2021-35393 MISC MISC MISC
realtek -- jungle_sdk	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-	2021-08-16	not yet calculated	CVE-2021-35395 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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 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.			
redos -- redos	User controlled `request.getHeader("Referer")`, `request.getRequestURL()` and	2021-08-18	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`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.		calculated	33580 MISC MLIST
rukovoditel -- project_management_app	An exploitable SQL injection vulnerability exists in the ‘entities/fields’ page of the Rukovoditel Project Management App 2.7.2. The heading_field_id parameter in ‘‘entities/fields’ page is vulnerable to authenticated SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability, this can be done either with administrator credentials or through cross-site request forgery.	2021-08-17	not yet calculated	CVE-2020-13588 MISC
rukovoditel -- project_management_app	An exploitable SQL injection vulnerability exists in the ‘entities/fields’ page of the Rukovoditel Project Management App 2.7.2. The entities_id parameter in the 'entities/fields page (mulitple_edit or copy_selected or export function) is vulnerable to authenticated SQL injection. An attacker can make	2021-08-17	not yet calculated	CVE-2020-13589 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated HTTP requests to trigger this vulnerability, this can be done either with administrator credentials or through cross-site request forgery.			
s/gmail -- s/gmail	In s/qmail through 4.0.07, an active MitM can inject arbitrary plaintext commands into a STARTTLS encrypted session between an SMTP client and s/qmail. This allows e-mail messages and user credentials to be sent to the MitM attacker.	2021-08-17	not yet calculated	CVE-2020-15955 MISC MISC
safecurl -- safecurl	SafeCurl before 0.9.2 has a DNS rebinding vulnerability.	2021-08-20	not yet calculated	CVE-2020-36474 MISC MISC
seacms -- seacms	Cross Site Request Forgery (CSRF) vulnerability exists in SeaCMS 10.7 in admin_manager.php, which could let a malicious user add an admin account.	2021-08-17	not yet calculated	CVE-2020-28846 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
seacms -- seacms	Cross Site Scripting (XSS) vulnerability exists in SeaCMS 12.6 via the (1) v_company and (2) v_tvs parameters in /admin_video.php,	2021-08-17	not yet calculated	CVE-2021-29313 MISC
seacms -- v210530	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=".	2021-08-18	not yet calculated	CVE-2021-37358 MISC
search_engine_management)system_project -- search_engine_management)system_project	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.	2021-08-19	not yet calculated	CVE-2021-28000 MISC
search_engine_management)system_project -- search_engine_management_system_project	A SQL injection vulnerability was discovered in the editid parameter in Local Services Search Engine Management System Project 1.0. This vulnerability gives admin users the ability to dump all data from the database.	2021-08-19	not yet calculated	CVE-2021-27999 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
secureid -- integration_kit	In Ping Identity RSA SecurID Integration Kit before 3.2, user impersonation can occur.	2021-08-18	not yet calculated	CVE-2021-39270 CONFIRM MISC
seopanel -- seopanel	A remote code execution vulnerability in SEOPanel 4.6.0 has been fixed for 4.7.0. This vulnerability allowed for remote code execution through an authenticated file upload via the Settings Panel>Import website function.	2021-08-20	not yet calculated	CVE-2020-27461 MISC MISC MISC
shopware -- shopware	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.	2021-08-16	not yet calculated	CVE-2021-37710 CONFIRM MISC
shopware -- shopware	Shopware is an open source eCommerce platform. Versions prior to 6.4.3.1 contain a vulnerability involving an insecure direct object reference of log	2021-08-16	not yet	CVE-2021-37709

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.		calculated	CONFIRM MISC
shopware -- shopware	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.	2021-08-16	not yet calculated	CVE-2021-37707 CONFIRM MISC
shopware -- shopware	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.	2021-08-16	not yet calculated	CVE-2021-37708 MISC CONFIRM
simple_image -- web_app	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.	2021-08-16	not yet calculated	CVE-2021-38753 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sinema -- remote_connect_client	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.	2021-08-19	not yet calculated	CVE-2021-31338 MISC
skycaiji -- skycaiji	Directory Traversal in Skycaiji v1.3 allows remote attackers to obtain sensitive information via the component 'index.php?m=admin&c=Tool&a=log&file=D%3A%5CphpStudy%5CWWW%5Cindex.php'.	2021-08-20	not yet calculated	CVE-2020-18878 MISC
smartertools -- smartermail	An issue was discovered in SmarterTools SmarterMail through 100.0.7537. Meddler-in-the-middle attackers can pipeline commands after a POP3 STLS command, injecting plaintext commands into an encrypted user session.	2021-08-17	not yet calculated	CVE-2020-29548 MISC MISC
sourcecodestar -- sourcecodestar	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.	2021-08-16	not yet calculated	CVE-2021-38752 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
suitecrm -- suitecrm	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) are not blocked.	2021-08-18	not yet calculated	CVE-2021-39267 MISC MISC MISC
suitecrm -- suitecrm	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.	2021-08-18	not yet calculated	CVE-2021-39268 MISC MISC MISC
tastyignighter -- tastyignighter	TastyIgniter 3.0.7 allows XSS via /account, /reservation, /admin/dashboard, and /admin/system_logs.	2021-08-15	not yet calculated	CVE-2021-38699 MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
textpattern -- textpattern	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.	2021-08-19	not yet calculated	CVE-2021-28001 MISC
textpattern -- textpattern	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.	2021-08-19	not yet calculated	CVE-2021-28002 MISC MISC
totolink -- a3002r	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.	2021-08-20	not yet calculated	CVE-2021-34223 MISC
totolink -- a3002r	Cross-site scripting in parent_control.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to	2021-08-20	not yet calculated	CVE-2021-34228 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execute arbitrary JavaScript by modifying the "Description" field and "Service Name" field.			
totolink -- a3002r	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.	2021-08-20	not yet calculated	CVE-2021-34220 MISC
totolink -- a3002r	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.	2021-08-20	not yet calculated	CVE-2021-34215 MISC
totolink -- a3002r	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.	2021-08-20	not yet calculated	CVE-2021-34207 MISC
totolink -- a702r	Directory Indexing in Login Portal of Login Portal of TOTOLINK-A702R-V1.0.0-B20161227.1023 allows	2021-08-20	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to access /add/ , /img/, /js/, and /mobile directories via GET Parameter.		calculated	34218 MISC
tp-link -- wireless_n_router_wr840n	In TP-Link Wireless N Router WR840N an ARP poisoning attack can cause buffer overflow	2021-08-19	not yet calculated	CVE-2021-29280 MISC MISC
tp-shop -- tp-shop	SQL Injection vulnerability exists in tp-shop 2.x-3.x via the /index.php/home/api/shop fBill parameter.	2021-08-17	not yet calculated	CVE-2020-18164 MISC
tranquil -- wapt	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.	2021-08-16	not yet calculated	CVE-2021-38608 MISC MISC
trim-off-newlines -- trim-off-newlines	All versions of package trim-off-newlines are vulnerable to Regular Expression Denial of Service (ReDoS) via string processing.	2021-08-18	not yet	CVE-2021-23425

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
			calculated	MISC MISC MISC
typora -- typora	Cross Site Scripting (XSS) in Typora v0.9.65 allows attackers to execute arbitrary code via mathjax syntax due to a mathjax configuration error in the mathematical formula blocks. This is a different vulnerability from CVE-2020-18221.	2021-08-19	not yet calculated	CVE-2020-18748 MISC MISC
ubuntu -- hg8045q	There is a command injection vulnerability in the HG8045Q product. When the command-line interface is enabled, which is disabled by default, attackers with administrator privilege could execute part of commands.	2021-08-13	not yet calculated	CVE-2021-37028 MISC JVN
ucweb -- ucweb	UCWeb UC 12.12.3.1219 through 12.12.3.1226 uses cleartext HTTP, and thus man-in-the-middle attackers can discover visited URLs.	2021-08-14	not yet calculated	CVE-2020-36473 MISC
vehicle_parking_management_system --	A persistent cross site scripting (XSS) vulnerability in the Add Categories module of Vehicle Parking	2021-08-19	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vehicle_parking_management_system	Management System 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the Category field.		calculated	27822 MISC
webrecorder -- pywb	Webrecorder pywb before 2.6.0 allows XSS because it does not ensure that Jinja2 templates are autoescaped.	2021-08-18	not yet calculated	CVE-2021-39286 MISC MISC
webtereas -- webtereas	Path Traversal vulneraility exists in webTareas 2.0 via the extpath parameter in general_serv.php, which could let a malicious user read arbitrary files.	2021-08-18	not yet calculated	CVE-2020-23069 MISC
wordpress -- wordpress	The Wonder Video Embed WordPress plugin before 1.8 does not escape parameters of its wonderplugin_video shortcode, which could allow users with a role as low as Contributor to perform Stored XSS attacks.	2021-08-16	not yet calculated	CVE-2021-24540 MISC
wordpress -- wordpress	The PhoneTrack Meu Site Manager WordPress plugin through 0.1 does not sanitise or escape its	2021-08-16	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	"php_id" setting before outputting it back in an attribute in the page, leading to a stored Cross-Site Scripting issue.		calculated	24534 MISC
wordpress -- wordpress	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 change them to arbitrary values.	2021-08-16	not yet calculated	CVE-2021-24380 MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-24538 MISC
wordpress -- wordpress	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.	2021-08-19	not yet calculated	CVE-2021-34645 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	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 inject arbitrary web scripts, in versions up to and including 0.1.5.	2021-08-16	not yet calculated	CVE-2021-34663 MISC MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-24548 MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34643 MISC MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-24512 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34658 MISC MISC
wordpress -- wordpress	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 inject arbitrary web scripts, in versions up to and including 1.0.	2021-08-16	not yet calculated	CVE-2021-34654 MISC MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34653 MISC MISC
wordpress -- wordpress	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	2021-08-16	not yet calculated	CVE-2021-34652

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	inject arbitrary web scripts, in versions up to and including 0.0.4.			MISC MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-38315 MISC MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34641 MISC MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34649 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34651 MISC MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34666 MISC MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34664 MISC MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34644 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34665 MISC MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34642 MISC MISC
wordpress -- wordpress	The WP Songbook WordPress 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.	2021-08-16	not yet calculated	CVE-2021-34655 MISC MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34659 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-34657 MISC MISC
wordpress -- wordpress	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	2021-08-16	not yet calculated	CVE-2021-24362 MISC
wordpress -- wordpress	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	2021-08-16	not yet calculated	CVE-2021-24518 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-24541 MISC
wordpress -- wordpress	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	2021-08-16	not yet calculated	CVE-2021-24363 MISC
wordpress -- wordpress	The à°¤à±†à°²à±?à°—à±? à°¬à±ˆà°¬à°¿à²²à±? 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 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	2021-08-16	not yet calculated	CVE-2021-24410 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The 2Way VideoCalls and 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.	2021-08-16	not yet calculated	CVE-2021-34656 MISC MISC
wordpress -- wordpress	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	2021-08-16	not yet calculated	CVE-2021-24445 MISC
wordpress -- wordpress	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	2021-08-16	not yet calculated	CVE-2021-24466 MISC
wordpress -- wordpress	The Social Tape WordPress plugin through 1.0 does not have CSRF checks in place when saving its	2021-08-16	not yet	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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		calculated	24411 MISC
wordpress -- wordpress	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).	2021-08-16	not yet calculated	CVE-2021-24471 MISC
wordpress -- wordpress	The Calendar_plugin WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of `$_SERVER['PHP_SELF']` in the ~/calendar.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.	2021-08-16	not yet calculated	CVE-2021-34667 MISC MISC
wordpress -- wordpress	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	2021-08-16	not yet calculated	CVE-2021-24519 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	admin to use XSS payload in it, leading to an authenticated Stored Cross-Site Scripting issue			
wordpress -- wordpress	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	2021-08-16	not yet calculated	CVE-2021-24526 MISC
wordpress -- wordpress	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.	2021-08-16	not yet calculated	CVE-2021-24527 MISC
wordpress -- wordpress	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	2021-08-16	not yet calculated	CVE-2021-24535 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Scripting payload in the Message Content. 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.			
wordpress -- wordpress	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	2021-08-16	not yet calculated	CVE-2021-24536 MISC
wp -- cerber	WP Cerber before 8.9.3 allows bypass of /wp-json access control via a trailing ? character.	2021-08-19	not yet calculated	CVE-2021-37598 MISC MISC
wp -- cerber	WP Cerber before 8.9.3 allows MFA bypass via wordpress_logged_in_[hash] manipulation.	2021-08-19	not yet calculated	CVE-2021-37597 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wuzhi -- wuzhi	SQL Injection in Wuzhi CMS v4.1.0 allows remote attackers to obtain sensitive information via the 'flag' parameter in the component '/coreframe/app/order/admin/index.php'.	2021-08-20	not yet calculated	CVE-2020-18877 MISC
xerosecurity -- sn1per	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.	2021-08-19	not yet calculated	CVE-2021-39273 MISC MISC MISC
xerosecurity -- sn1per	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.	2021-08-19	not yet calculated	CVE-2021-39274 MISC MISC MISC
yclas -- yclas	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 parameter.	2021-08-18	not yet calculated	CVE-2021-38710 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zint -- barcode_generator	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.	2021-08-17	not yet calculated	CVE-2021-39247 MISC MISC
zstack -- zstack	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())	2021-08-17	not yet calculated	CVE-2021-32829 CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	GroovyInterceptor. Even though the sandbox heavily restricts the receiver types to a small set of allowed types, the sandbox is non effective at 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.			