Vulnerability Summary for the Week of September 20, 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
adobe -- digital_editions	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by an arbitrary command execution vulnerability. An authenticated attacker could leverage this vulnerability to execute arbitrary commands. User interaction is required to abuse this vulnerability in that a user must open a maliciously crafted .epub file.	2021-09-27	9.3	CVE-2021-39826 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- photoshop_2020	Adobe Photoshop versions 21.2.11 (and earlier) and 22.5 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted SVG 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.	2021-09-27	9.3	CVE-2021-40709 MISC
adobe -- premiere_elements	Adobe Premiere Elements version 2021.2235820 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious png file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-09-27	9.3	CVE-2021-39824 MISC
atlassian -- floodlight	Floodlight through 1.2 has poor input validation in checkFlow in StaticFlowEntryPusherResource.java because of undefined fields mishandling.	2021-09-30	7.5	CVE-2020-18683 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- floodlight	Floodlight through 1.2 has poor input validation in checkFlow in StaticFlowEntryPusherResource.java because of unchecked prerequisites related to TCP or UDP ports, or group or table IDs.	2021-09-30	7.5	CVE-2020-18685 MISC
concretecms -- concrete_cms	An issue was discovered in Concrete CMS through 8.5.5. Path Traversal leading to RCE via external form by adding a regular expression.	2021-09-27	7.5	CVE-2021-40098 MISC MISC
github -- enterprise_server	An improper access control vulnerability in GitHub Enterprise Server allowed a workflow job to execute in a self-hosted runner group it should not have had access to. This affects customers using self-hosted runner groups for access control. A repository with access to one enterprise runner group could access all of the enterprise runner groups within the organization because of improper authentication checks during the request. This could cause code to be run unintentionally by the incorrect runner group. This vulnerability affected GitHub Enterprise Server	2021-09-24	7.5	CVE-2021-22869 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	versions from 3.0.0 to 3.0.15 and 3.1.0 to 3.1.7 and was fixed in 3.0.16 and 3.1.8 releases.			
lodash -- lodash	** DISPUTED ** A command injection vulnerability in Lodash 4.17.21 allows attackers to achieve arbitrary code execution via the template function. This is a different parameter, method, and version than CVE-2021-23337. NOTE: the vendor's position is that it's the developer's responsibility to ensure that a template does not evaluate code that originates from untrusted input.	2021-09-30	7.5	CVE-2021-41720 MISC
microfocus -- arcsight_enterprise_security_manager	Remote Code Execution vulnerability in Micro Focus ArcSight Enterprise Security Manager (ESM) product, affecting versions 7.0.2 through 7.5. The vulnerability could be exploited resulting in remote code execution.	2021-09-28	7.5	CVE-2021-38124 MISC
nagios -- nagios_xi	Nagios XI before 5.8.5 has Incorrect Permission Assignment for repairmysql.sh.	2021-09-28	7.5	CVE-2021-36365

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM CONFIRM
nagios -- nagios_xi	Nagios XI before 5.8.5 has Incorrect Permission Assignment for migrate.php.	2021-09-28	7.5	CVE-2021-36363 CONFIRM CONFIRM
openvpn-monitor_project -- openvpn-monitor	furlongm openvpn-monitor through 1.1.3 allows %0a command injection via the OpenVPN management interface socket. This can shut down the server via signal%20SIGTERM.	2021-09-27	7.8	CVE-2021-31605 MISC MISC
oracle -- linux	Vulnerability in Oracle Linux (component: OSwatcher). Supported versions that are affected are 7 and 8. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Linux executes to compromise Oracle Linux. Successful attacks of this vulnerability can result in takeover of Oracle Linux. CVSS 3.1 Base	2021-09-24	7.2	CVE-2021-2464 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).			
phoenixcontact -- plcnext_technology_starterkit_firmware	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.	2021-09-27	7.8	CVE-2021-34570 CONFIRM
set_user_project -- set_user	The set_user extension module before 3.0.0 for PostgreSQL allows ProcessUtility_hook bypass via set_config.	2021-09-27	7.5	CVE-2021-41558 CONFIRM
skale -- sgxwallet	An issue was discovered in SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address is then freed, resulting in compromised integrity of the enclave. This was	2021-09-27	7.5	CVE-2021-36219 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	resolved after v1.58.3 and not reproducible in sgxwallet v1.77.0.			
stylemixthemes -- ulisting	Unauthenticated Privilege Escalation vulnerability in WordPress uListing plugin (versions <= 2.0.5). Possible if WordPress configuration allows user registration.	2021-09-27	7.5	CVE-2021-36879 MISC CONFIRM
stylemixthemes -- ulisting	Unauthenticated SQL Injection (SQLi) vulnerability in WordPress uListing plugin (versions <= 2.0.3), vulnerable parameter: custom.	2021-09-27	7.5	CVE-2021-36880 MISC CONFIRM
surelinesystems -- sureedge_migrator	A SQL injection vulnerability exists in Sureline SUREedge Migrator 7.0.7.29360.	2021-09-28	7.5	CVE-2021-38303 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
trendmicro -- serverprotect	A vulnerability in Trend Micro ServerProtect for Storage 6.0, ServerProtect for EMC Celerra 5.8, ServerProtect for Network Appliance Filers 5.8, and ServerProtect for Microsoft Windows / Novell Netware 5.8 could allow a remote attacker to bypass authentication on affected installations.	2021-09-29	10	CVE-2021-36745 MISC MISC MISC
zohocorp -- manageengine_admanager_plus	Zoho ManageEngine ADManager Plus version 7110 and prior is vulnerable to unrestricted file upload, leading to remote code execution.	2021-09-27	7.5	CVE-2021-37761 MISC MISC
zohocorp -- manageengine_admanager_plus	Zoho ManageEngine ADManager Plus before 7111 is vulnerable to unrestricted file which leads to Remote code execution.	2021-09-27	7.5	CVE-2021-37539 MISC MISC
zyxel -- zywall_vpn2s_firmware	A command injection vulnerability in the CGI program of the Zyxel VPN2S firmware version 1.12	2021-09-29	7.2	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could allow an authenticated, local user to execute arbitrary OS commands.			35028 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- creative_cloud_desktop_application	Adobe Creative Cloud Desktop Application for macOS version 5.3 (and earlier) is affected by a privilege escalation vulnerability that could allow a normal user to delete the OOBE directory and get permissions of any directory under the administrator authority.	2021-09-29	4.6	CVE-2021-28547 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- digital_editions	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by a privilege escalation vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to escalate privileges. User interaction is required before product installation to abuse this vulnerability.	2021-09-27	6.8	CVE-2021-39828 MISC
adobe -- digital_editions	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by an arbitrary file write vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to write an arbitrary file to the system. User interaction is required before product installation to abuse this vulnerability.	2021-09-27	6.8	CVE-2021-39827 MISC
adobe -- experience_manager	Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a stored XSS vulnerability when creating Content Fragments. An authenticated attacker can send a malformed POST request to achieve	2021-09-27	4.3	CVE-2021-40711 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	server-side denial of service. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.			
adobe -- experience_manager	Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a improper input validation vulnerability via the path parameter. An authenticated attacker can send a malformed POST request to achieve server-side denial of service.	2021-09-27	4	CVE-2021-40712 MISC
adobe -- experience_manager	Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a improper certificate validation vulnerability in the cold storage component. If an attacker can achieve a man in the middle when the cold server establishes a new certificate, they would be able to harvest sensitive information.	2021-09-27	4.3	CVE-2021-40713 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- experience_manager	Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability via the accesskey parameter. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser	2021-09-27	4.3	CVE-2021-40714 MISC
adobe -- incopy	Adobe InCopy version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious TIFF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	2021-09-27	6.8	CVE-2021-39818 MISC
adobe -- incopy	Adobe InCopy version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious XML file, potentially resulting in arbitrary code execution in the context of	2021-09-27	6.8	CVE-2021-39819 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the current user. User interaction is required to exploit this vulnerability.			
adobe -- indesign	Adobe InDesign versions 16.3 (and earlier), and 16.3.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious TIF file.	2021-09-29	6.8	CVE-2021-39821 MISC
apache -- druid	In the Druid ingestion system, the InputSource is used for reading data from a certain data source. However, the HTTP InputSource allows authenticated users to read data from other sources than intended, such as the local file system, with the privileges of the Druid server process. This is not an elevation of privilege when users access Druid directly, since Druid also provides the Local InputSource, which allows the same level of access. But it is problematic when users interact with Druid	2021-09-24	4	CVE-2021-36749 MISC MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	indirectly through an application that allows users to specify the HTTP InputSource, but not the Local InputSource. In this case, users could bypass the application-level restriction by passing a file URL to the HTTP InputSource. This issue was previously mentioned as being fixed in 0.21.0 as per CVE-2021-26920 but was not fixed in 0.21.0 or 0.21.1.			
asus -- armoury_crate_lite_service	ASUS ROG Armoury Crate Lite before 4.2.10 allows local users to gain privileges by placing a Trojan horse file in the publicly writable %PROGRAMDATA%\ASUS\GamingCenterLib directory.	2021-09-27	4.4	CVE-2021-40981 MISC
concretecms -- concrete_cms	An issue was discovered in Concrete CMS through 8.5.5. Authenticated path traversal leads to to remote code execution via uploaded PHP code, related to the bFilename parameter.	2021-09-27	6.5	CVE-2021-40097 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
concretecms -- concrete_cms	An issue was discovered in Concrete CMS through 8.5.5. There is unauthenticated stored XSS in blog comments via the website field.	2021-09-27	4.3	CVE-2021-40106 MISC MISC
concretecms -- concrete_cms	An issue was discovered in Concrete CMS through 8.5.5. There is XSS via Markdown Comments.	2021-09-27	4.3	CVE-2021-40105 MISC MISC
concretecms -- concrete_cms	An issue was discovered in Concrete CMS through 8.5.5. There is an SVG sanitizer bypass.	2021-09-27	5	CVE-2021-40104 MISC MISC
concretecms -- concrete_cms	A SSRF issue was discovered in Concrete CMS through 8.5.5. Users can access forbidden files on their local network. A user with permissions to upload files from	2021-09-27	5.5	CVE-2021-40109

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	external sites can upload a URL that redirects to an internal resource of any file type. The redirect is followed and loads the contents of the file from the redirected-to server. Files of disallowed types can be uploaded.			MISC MISC
concretecms -- concrete_cms	An issue was discovered in Concrete CMS through 8.5.5. Arbitrary File deletion can occur via PHAR deserialization in is_dir (PHP Object Injection associated with the __wakeup magic method).	2021-09-24	6.4	CVE-2021-40102 MISC MISC
concretecms -- concrete_cms	An issue was discovered in Concrete CMS through 8.5.5. Fetching the update json scheme over HTTP leads to remote code execution.	2021-09-24	6.5	CVE-2021-40099 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
concretecms -- concrete_cms	An issue was discovered in Concrete CMS through 8.5.5. Path Traversal can lead to Arbitrary File Reading and SSRF.	2021-09-27	5	CVE-2021-40103 MISC MISC
concretecms -- concrete_cms	An issue was discovered in Concrete CMS through 8.5.5. The Calendar is vulnerable to CSRF. ccm_token is not verified on the ccm/calendar/dialogs/event/add/save endpoint.	2021-09-27	6.8	CVE-2021-40108 MISC MISC
couchbase -- couchbase_server	Couchbase Server 6.5.x, 6.6.x through 6.6.2, and 7.0.0 has a Buffer Overflow. A specially crafted network packet sent from an attacker can crash memcached.	2021-09-29	5	CVE-2021-35944 MISC MISC
couchbase -- couchbase_server	Couchbase Server 6.5.x, 6.6.0 through 6.6.2, and 7.0.0, has a Buffer Overflow. A	2021-09-29	5	CVE-2021-35945

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	specially crafted network packet sent from an attacker can crash memcached.			MISC MISC
d-link -- dcs-932l_firmware	** UNSUPPORTED WHEN ASSIGNED ** DCS-5000L v1.05 and DCS-932L v2.17 and older are affecged by Incorrect Acess Control. The use of the basic authentication for the devices command interface allows attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-09-24	5.2	CVE-2021-41503 MISC MISC
d-link -- dcs-932l_firmware	** UNSUPPORTED WHEN ASSIGNED ** An Elevated Privileges issue exists in D-Link DCS-5000L v1.05 and DCS-932L v2.17 and older. The use of the digest-authentication for the devices command interface may allow further attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access	2021-09-24	5.2	CVE-2021-41504 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.			
dell -- emc_networker	Dell NetWorker, versions 18.x and 19.x contain a Path traversal vulnerability. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and gain access to unauthorized information.	2021-09-28	4	CVE-2021-21569 MISC
dell -- emc_networker	Dell NetWorker, versions 18.x and 19.x contain an Information disclosure vulnerability. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and gain access to unauthorized information.	2021-09-28	4	CVE-2021-21570 MISC
dlink -- dir-605l_firmware	An informtion disclosure issue exists in D-LINK-DIR-605 B2 Firmware Version : 2.01MT. An attacker can obtain a user	2021-09-24	5	CVE-2021-40655

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	name and password by forging a post request to the / getcfg.php page			MISC MISC
dlink -- dir-615_firmware	An information disclosure issue exist in D-LINK-DIR-615 B2 2.01mt. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page	2021-09-24	4	CVE-2021-40654 MISC MISC
firefly-iii -- firefly_iii	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF)	2021-09-27	6.8	CVE-2021-3819 CONFIRM MISC
getgrav -- grav	grav is vulnerable to Reliance on Cookies without Validation and Integrity Checking	2021-09-27	5	CVE-2021-3818 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
getgrav -- grav-plugin-admin	grav-plugin-admin is vulnerable to Improper Restriction of Rendered UI Layers or Frames	2021-09-27	5.8	CVE-2021-3799 CONFIRM MISC
gilacms -- gila_cms	A Cross-Site Request Forgery (CSRF) in GilaCMS v1.11.4 allows authenticated attackers to arbitrarily add administrator accounts.	2021-09-27	6.8	CVE-2020-20693 MISC
gilacms -- gila_cms	GilaCMS v1.11.4 was discovered to contain a SQL injection vulnerability via the $_GET parameter in /src/core/controllers/cm.php.	2021-09-27	6.5	CVE-2020-20692 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
github -- enterprise_server	A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to read files on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.1.8 and was fixed in 3.1.8, 3.0.16, and 2.22.22. This vulnerability was reported via the GitHub Bug Bounty program. This is the result of an incomplete fix for CVE-2021-22867.	2021-09-24	4	CVE-2021-22868 MISC MISC MISC
google -- android	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	2021-09-27	4.6	CVE-2021-0611 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.			
google -- android	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	2021-09-27	4.6	CVE-2021-0610 MISC
google -- android	In ccu, there is a possible out of bounds read due to incorrect error handling. This could lead to information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827145; Issue ID: ALPS05827145.	2021-09-27	4	CVE-2021-0660 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	2021-09-27	4.6	CVE-2021-0612 MISC
gradle -- gradle	In Gradle Enterprise before 2021.1.3, an attacker with the ability to perform SSRF attacks can potentially reset the system user password.	2021-09-24	5	CVE-2021-41586 MISC
gradle -- gradle	Gradle Enterprise before 2021.1.3 can allow unauthorized viewing of a response (information disclosure of possibly sensitive build/configuration details) via a crafted HTTP request with the X-Gradle-Enterprise-Ajax-Request header.	2021-09-24	5	CVE-2021-41584 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gradle -- gradle	In Gradle Enterprise before 2021.1.3, an attacker with the ability to perform SSRF attacks can potentially discover credentials for other resources.	2021-09-24	5	CVE-2021-41587 MISC
gradle -- gradle	In Gradle Enterprise before 2021.1.3, a crafted request can trigger deserialization of arbitrary unsafe Java objects. The attacker must have the encryption and signing keys.	2021-09-24	6.8	CVE-2021-41588 MISC
ibm -- sterling_order_management	IBM Sterling Order Management 9.4, 9.5, and 10.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199179.	2021-09-30	4.3	CVE-2021-20554 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
inflect_project -- inflect	inflect is vulnerable to Inefficient Regular Expression Complexity	2021-09-27	5	CVE-2021-3820 MISC CONFIRM
jsoneditoronline -- jsoneditor	jsoneditor is vulnerable to Inefficient Regular Expression Complexity	2021-09-27	5	CVE-2021-3822 MISC CONFIRM
kindsoft -- kindeditor	Cross Site Scripting (XSS) vulnerability exists in all versions of KindEditor, which can be exploited by an attacker to obtain user cookie information.	2021-09-28	4.3	CVE-2021-37267 MISC
kindsoft -- kindeditor	Cross Site Scripting (XSS) vulnerability exists in KindEditor (Chinese versions) 4.1.12,	2021-09-28	4.3	CVE-2021-30086

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	which can be exploited by an attacker to obtain user cookie information.			MISC MISC
laracms_project -- laracms	LaraCMS v1.0.1 transmits sensitive information in cleartext which can be intercepted by attackers.	2021-09-29	5	CVE-2020-20128 MISC
maccms -- maccms	A Cross-Site Request Forgery (CSRF) in Maccms v10 via admin.php/admin/admin/del/ids/<id>.html allows authenticated attackers to delete all users.	2021-09-24	4.9	CVE-2020-20514 MISC
nltk -- nltk	nltk is vulnerable to Inefficient Regular Expression Complexity	2021-09-27	5	CVE-2021-3828 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openbsd -- libressl	x509_constraints_parse_mailbox in lib/libcrypto/x509/x509_constraints.c in LibreSSL through 3.4.0 has a stack-based buffer over-read. When the input exceeds DOMAIN_PART_MAX_LEN, the buffer lacks '\0' termination.	2021-09-24	4.3	CVE-2021-41581 MISC
openbsd -- openssh	sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.	2021-09-26	6	CVE-2021-41617 MISC MISC MISC CONFIRM FEDORA FEDORA
opennms -- opennms	OpenNMS version 18.0.1 and prior are vulnerable to a stored XSS issue due to insufficient filtering of SNMP agent supplied data. By creating a malicious	2021-09-24	4.3	CVE-2016-6556

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	SNMP 'sysName' or 'sysContact' response, an attacker can store an XSS payload which will trigger when a user of the web UI views the data. This issue was fixed in version 18.0.2, released on September 20, 2016.			MISC MISC
opennms -- opennms	OpenNMS version 18.0.1 and prior are vulnerable to a stored XSS issue due to insufficient filtering of SNMP trap supplied data. By creating a malicious SNMP trap, an attacker can store an XSS payload which will trigger when a user of the web UI views the events list page. This issue was fixed in version 18.0.2, released on September 20, 2016.	2021-09-24	4.3	CVE-2016-6555 MISC MISC
openvpn-monitor_project -- openvpn-monitor	furlongm openvpn-monitor through 1.1.3 allows Authorization Bypass to disconnect arbitrary clients.	2021-09-27	5	CVE-2021-31606 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openvpn-monitor_project -- openvpn-monitor	furlongm openvpn-monitor through 1.1.3 allows CSRF to disconnect an arbitrary client.	2021-09-27	4.3	CVE-2021-31604 MISC MISC
os4ed -- opensis	A SQL injection vulnerability exists in the Take Attendance functionality of OS4Ed's OpenSIS 8.0. allows an attacker to inject their own SQL query. The cp_id_miss_attn parameter from TakeAttendance.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request as a user with access to "Take Attendance" functionality to trigger this vulnerability.	2021-09-24	6.5	CVE-2021-40309 MISC MISC MISC
pingidentity -- pingaccess	Ping Identity PingAccess before 5.3.3 allows HTTP request smuggling via header manipulation.	2021-09-24	5	CVE-2021-31923 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
shopkit_project -- shopkit	Shopkit v2.7 contains a reflective cross-site scripting (XSS) vulnerability in the /account/register component, which allows attackers to hijack user credentials via a crafted payload in the E-Mail text field.	2021-09-24	4.3	CVE-2020-20508 MISC
siemens -- solid_edge	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13789).	2021-09-28	6.8	CVE-2021-41537 MISC MISC
siemens -- solid_edge	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to information disclosure by unexpected access to an uninitialized pointer while parsing user-supplied OBJ files. An attacker could leverage this vulnerability to leak	2021-09-28	4.3	CVE-2021-41538 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	information from unexpected memory locations (ZDI-CAN-13770).			
siemens -- solid_edge	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process (ZDI-CAN-13703).	2021-09-28	4.3	CVE-2021-41534 MISC MISC
siemens -- solid_edge	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process (ZDI-CAN-13565).	2021-09-28	4.3	CVE-2021-41533 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- solid_edge	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13778).	2021-09-28	6.8	CVE-2021-41536 MISC MISC
siemens -- solid_edge	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13771).	2021-09-28	6.8	CVE-2021-41535 MISC MISC
siemens -- solid_edge	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this	2021-09-28	6.8	CVE-2021-41540 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability to execute code in the context of the current process (ZDI-CAN-13776).			
siemens -- solid_edge	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13773).	2021-09-28	6.8	CVE-2021-41539 MISC MISC
skale -- sgxwallet	An issue was discovered in SKALE sgxwallet 1.58.3. sgx_disp_ippsAES_GCMEncrypt allows an out-of-bounds write, resulting in a segfault and compromised enclave. This issue describes a buffer overflow, which was resolved prior to v1.77.0 and not reproducible in latest sgxwallet v1.77.0	2021-09-27	5	CVE-2021-36218 MISC MISC
speed_test_project -- speed_test	e7d Speed Test (aka speedtest) 0.5.3 allows a path-traversal attack that results in	2021-09-27	5	CVE-2021-40349

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	information disclosure via the "GET /.." substring.			MISC MISC
spotweb_project -- spotweb	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the firstname parameter.	2021-10-01	4.3	CVE-2021-40969 MISC MISC
streama_project -- streama	A cross-site request forgery (CSRF) vulnerability exists in Streama up to and including v1.10.3. The application does not have CSRF checks in place when performing actions such as uploading local files. As a result, attackers could make a logged-in administrator upload arbitrary local files via a CSRF attack and send them to the attacker.	2021-09-29	6.8	CVE-2021-41764 MISC MISC MISC
stylemixthemes -- ulisting	Authenticated Insecure Direct Object References (IDOR) vulnerability in	2021-09-27	6.5	CVE-2021-36874

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WordPress uListing plugin (versions <= 2.0.5).			MISC CONFIRM
stylemixthemes -- ulisting	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in WordPress uListing plugin (versions <= 2.0.5) as it lacks CSRF checks on plugin administration pages.	2021-09-27	6.8	CVE-2021-36876 MISC CONFIRM
stylemixthemes -- ulisting	Cross-Site Request Forgery (CSRF) vulnerability in WordPress uListing plugin (versions <= 2.0.5) makes it possible for attackers to modify user roles.	2021-09-27	4.3	CVE-2021-36877 MISC CONFIRM
trendmicro -- housecall_for_home_networks	An uncontrolled search path element privilege escalation vulnerability in Trend Micro HouseCall for Home Networks version 5.3.1225 and below could allow an	2021-09-29	6.9	CVE-2021-32466 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to escalate privileges by placing a custom crafted file in a specific directory to load a malicious library. Please note that an attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.			MISC MISC
wpdevart -- countdown_and_countup\,_woocommerce_sales_timer	The Countdown and CountUp, WooCommerce Sales Timers WordPress plugin is vulnerable to Cross-Site Request Forgery via the save_theme function found in the ~/includes/admin/coundown_theme_page.php file due to a missing nonce check which allows attackers to inject arbitrary web scripts, in versions up to and including 1.5.7.	2021-09-28	6.8	CVE-2021-34636 MISC MISC
wpxpo -- postx_-_gutenberg_blocks_for_post_grid	The PostX â€“ Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10 performs incorrect checks before allowing any logged in user to perform some ajax	2021-09-27	4	CVE-2021-24652 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	based requests, allowing any user to modify, delete or add ultp_options values.			
zte -- axon_30_pro_message_service	There is an information leak vulnerability in the message service app of a ZTE mobile phone. Due to improper parameter settings, attackers could use this vulnerability to obtain some sensitive information of users by accessing specific pages.	2021-09-25	4.3	CVE-2021-21742 MISC
zyxel -- zywall_vpn2s_firmware	A directory traversal vulnerability in the web server of the Zyxel VPN2S firmware version 1.12 could allow a remote attacker to gain access to sensitive information.	2021-09-29	5	CVE-2021-35027 MISC