Vulnerability Summary for the Week of August 9, 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
alg_ds_project -- alg_ds	An issue was discovered in the alg_ds crate through 2020-08-25 for Rust. There is a drop of uninitialized memory in Matrix::new().	2021-08-08	7.5	CVE-2020-36432 MISC MISC
care2x -- hospital_information_management_system	SQL Injection Vulnerability in Care2x Open Source Hospital Information Management 2.7 Alpha via the (1) pday, (2) pmonth, and (3) pyear	2021-08-06	7.5	CVE-2021-36351 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameters in GET requests sent to /modules/nursing/nursing-station.php.			
dell -- openmanage_enterprise	Dell OpenManage Enterprise versions prior to 3.6.1 contain an improper authentication vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability to hijack an elevated session or perform unauthorized actions by sending malformed data.	2021-08-09	7.5	CVE-2021-21564 CONFIRM
dell -- openmanage_enterprise	Dell OpenManage Enterprise versions prior to 3.6.1 contain an OS command injection vulnerability in RACADM and IPMI tools. A remote authenticated malicious user with high privileges may potentially exploit this vulnerability to execute arbitrary OS commands.	2021-08-09	9	CVE-2021-21585 CONFIRM
dlink -- dir-615_firmware	A buffer overflow in D-Link DIR-615 C2 3.03WW. The ping_ipaddr parameter in ping_response.cgi POST request allows an attacker to crash the	2021-08-06	7.5	CVE-2021-37388 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	webserver and might even gain remote code execution.			
dreamsecurity -- magicline4nx.exe	A vulnerability in PKI Security Solution of Dream Security could allow arbitrary command execution. This vulnerability is due to insufficient validation of the authorization certificate. An attacker could exploit this vulnerability by sending a crafted HTTP request an affected program. A successful exploit could allow the attacker to remotely execute arbitrary code on a target system.	2021-08-06	10	CVE-2021-26606 MISC
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows memory corruption during conversion of a PDF document to a different document format.	2021-08-11	7.5	CVE-2021-38568 MISC
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows SQL Injection via crafted data at the end of a string.	2021-08-11	7.5	CVE-2021-38574 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxitsoftware -- foxit_reader	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 have an out-of-bounds write because the Cross-Reference table is mishandled during Office document conversion.	2021-08-11	7.5	CVE-2021-33793 MISC
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows writing to arbitrary files because a CombineFiles pathname is not validated.	2021-08-11	7.5	CVE-2021-38573 MISC
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows writing to arbitrary files because the extractPages pathname is not validated.	2021-08-11	7.5	CVE-2021-38572 MISC
gestionaleamica -- amica_prodigy	A vulnerability was found in CIR 2000 / Gestionale Amica Prodigy v1.7. The Amica Prodigy's executable "RemoteBackup.Service.exe" has incorrect permissions, allowing a local unprivileged user to replace it with a malicious file that will be executed with "LocalSystem" privileges.	2021-08-06	7.2	CVE-2021-35312 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jeecg -- jeecg_boot	An arbitrary file upload vulnerability in /jeecg-boot/sys/common/upload of jeecg-boot CMS 2.3 allows attackers to execute arbitrary code.	2021-08-06	7.5	CVE-2020-28088 MISC
jetbrains -- hub	In JetBrains Hub before 2021.1.13389, account takeover was possible during password reset.	2021-08-06	7.5	CVE-2021-36209 MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.4, there was an insecure deserialization.	2021-08-06	7.5	CVE-2021-37544 MISC
linux -- linux_kernel	In drivers/char/virtio_console.c in the Linux kernel before 5.13.4, data corruption or loss can be triggered by an untrusted device that supplies a buf->len value exceeding the buffer size.	2021-08-07	7.2	CVE-2021-38160 MISC MISC
obsdian -- obsidian	Obsidian before 0.12.12 does not require user confirmation for non-http/https URLs.	2021-08-07	7.5	CVE-2021-38148 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
progress -- moveit_transfer	In certain Progress MOVEit Transfer versions before 2021.0.4 (aka 13.0.4), SQL injection in the MOVEit Transfer web application could allow an unauthenticated remote attacker to gain access to the database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, or execute SQL statements that alter or delete database elements, via crafted strings sent to unique MOVEit Transfer transaction types. The fixed versions are 2019.0.8 (11.0.8), 2019.1.7 (11.1.7), 2019.2.4 (11.2.4), 2020.0.7 (12.0.7), 2020.1.6 (12.1.6), and 2021.0.4 (13.0.4).	2021-08-07	7.5	CVE-2021-38159 CONFIRM MISC
prolink -- prc2402m_firmware	In ProLink PRC2402M V1.0.18 and older, the set_sys_cmd function in the adm.cgi binary, accessible with a page parameter value of sysCMD contains a trivial command injection where the value of the command parameter is passed directly to system.	2021-08-06	7.5	CVE-2021-36706 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
prolink -- prc2402m_firmware	In ProLink PRC2402M V1.0.18 and older, the set_TR069 function in the adm.cgi binary, accessible with a page parameter value of TR069 contains a trivial command injection where the value of the TR069_local_port parameter is passed directly to system.	2021-08-06	7.5	CVE-2021-36705 MISC
prolink -- prc2402m_firmware	In ProLink PRC2402M V1.0.18 and older, the set_ledonoff function in the adm.cgi binary, accessible with a page parameter value of ledonoff contains a trivial command injection where the value of the led_cmd parameter is passed directly to do_system.	2021-08-06	7.5	CVE-2021-36707 MISC
rconfig -- rconfig	rConfig 3.9.5 allows command injection by sending a crafted GET request to lib/ajaxHandlers/ajaxArchiveFiles.php since the path parameter is passed directly to the exec function without being escaped.	2021-08-09	7.5	CVE-2020-23151 MISC
roxy-wi -- roxy-wi	Roxy-WI through 5.2.2.0 allows SQL Injection via check_login. An	2021-08-07	7.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthenticated attacker can extract a valid uuid to bypass authentication.			38167 MISC
sys-info_project -- sys-info	An issue was discovered in the sys-info crate before 0.8.0 for Rust. sys_info::disk_info calls can trigger a double free.	2021-08-08	7.5	CVE-2020-36434 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
comrak_project -- comrak	An issue was discovered in the comrak crate before 0.10.1 for Rust. It mishandles & characters, leading to XSS via &# HTML entities.	2021-08-08	4.3	CVE-2021-38186 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
corero -- securewatch_managed_services	Corero SecureWatch Managed Services 9.7.2.0020 is affected by a Path Traversal vulnerability via the snap_file parameter in the /it-IT/splunkd/__raw/services/get_snapshot HTTP API endpoint. A ‘low privileged’ attacker can read any file on the target host.	2021-08-06	4	CVE-2021-38136 MISC MISC
corero -- securewatch_managed_services	Corero SecureWatch Managed Services 9.7.2.0020 does not correctly check swa-monitor and cns-monitor user’s privileges, allowing a user to perform actions not belonging to his role.	2021-08-06	5.5	CVE-2021-38137 MISC MISC
ctparental_project -- ctparental	CTparental before 4.45.03 is vulnerable to cross-site scripting (XSS) in the CTparental admin panel. In bl_categires_help.php, the 'categories' variable is assigned with the content of the query string param 'cat' without sanitization or encoding, enabling an attacker to inject malicious code into the output webpage.	2021-08-10	4.3	CVE-2021-37365 MISC MISC
ctparental_project -- ctparental	CTparental before 4.45.03 is vulnerable to cross-site request forgery (CSRF) in the	2021-08-10	6.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CTparental admin panel. By combining CSRF with XSS, an attacker can trick the administrator into clicking a link that cancels the filtering for all standard users.			37366 MISC MISC
ctparental_project -- ctparental	CTparental before 4.45.07 is affected by a code execution vulnerability in the CTparental admin panel. Because The file "bl_categories_help.php" is vulnerable to directory traversal, an attacker can create a file that contains scripts and run arbitrary commands.	2021-08-10	4.6	CVE-2021-37367 MISC MISC
dell -- openmanage_enterprise	Dell OpenManage Enterprise version 3.5 and OpenManage Enterprise-Modular version 1.30.00 contain an information disclosure vulnerability. An authenticated low privileged attacker may potentially exploit this vulnerability leading to disclosure of the OIDC server credentials.	2021-08-09	4	CVE-2021-21584 CONFIRM
dell -- openmanage_enterprise	Dell OpenManage Enterprise versions 3.4 through 3.6.1 and Dell OpenManage Enterprise Modular versions 1.20.00 through	2021-08-09	5.8	CVE-2021-21596

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	1.30.00, contain a remote code execution vulnerability. A malicious attacker with access to the immediate subnet may potentially exploit this vulnerability leading to information disclosure and a possible elevation of privileges.			CONFIRM
fig2dev_project -- fig2dev	A stack-based buffer overflow in the genptk_text component in genptk.c of fig2dev 3.2.7b allows attackers to cause a denial of service (DOS) via converting a xfig file into ptk format.	2021-08-10	4.3	CVE-2020-21675 MISC
fortinet -- fortianalyzer	An improper access control vulnerability in FortiManager and FortiAnalyzer GUI interface 7.0.0, 6.4.5 and below, 6.2.8 and below, 6.0.11and below, 5.6.11and below may allow a remote and authenticated attacker with restricted user profile to retrieve the list of administrative users of other ADOMs and their related configuration.	2021-08-06	4	CVE-2021-32587 CONFIRM
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows attackers	2021-08-11	6.4	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to delete arbitrary files (during uninstallation) via a symlink.			38570 MISC
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows DLL hijacking, aka CNVD-C-2021-68000 and CNVD-C-2021-68502.	2021-08-11	4.4	CVE-2021-38571 MISC
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows stack consumption via recursive function calls during the handling of XFA forms or link objects.	2021-08-11	5	CVE-2021-38569 MISC
foxitsoftware -- foxit_reader	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 allow information disclosure or an application crash after mishandling the Tab key during XFA form interaction.	2021-08-11	6.4	CVE-2021-33794 MISC
ignitedcms_project -- ignitedcms	Cross Site Request Forgery (CSRF) in IgnitedCMS v1.0 allows remote attackers to obtain sensitive information and gain privilege	2021-08-06	6.8	CVE-2020-18694 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	via the component "/admin/profile/save_profile".			
intelliants -- subrion	Cross-Site Scripting (XSS) vulnerability in Subrion 4.2.1 via the title when adding a page.	2021-08-06	4.3	CVE-2020-22330 MISC
jeecg -- jeecg_boot	A SQL injection vulnerability in /jeecg boot/sys/dict/loadtreedata of jeecg-boot CMS 2.3 allows attackers to access sensitive database information.	2021-08-06	5	CVE-2020-28087 MISC
jetbrains -- hub	In JetBrains Hub before 2021.1.13402, HTML injection in the password reset email was possible.	2021-08-06	4.3	CVE-2021-37541 MISC
jetbrains -- hub	In JetBrains Hub before 2021.1.13262, a potentially insufficient CSP for the Widget deployment feature was used.	2021-08-06	6.4	CVE-2021-37540 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetbrains -- rubymine	In JetBrains RubyMine before 2021.1.1, code execution without user confirmation was possible for untrusted projects.	2021-08-06	6.5	CVE-2021-37543 MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2021.1, passwords in cleartext sometimes could be stored in VCS.	2021-08-06	5	CVE-2021-37548 MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2021.1, an insecure key generation mechanism for encrypted properties was used.	2021-08-06	5	CVE-2021-37546 MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.3, XSS was possible.	2021-08-06	4.3	CVE-2021-37542 MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.4, insufficient checks during file uploading were made.	2021-08-06	5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				37547 MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2021.1.1, insufficient authentication checks for agent requests were made.	2021-08-06	5	CVE-2021-37545 MISC
jetbrains -- youtrack	In JetBrains YouTrack before 2021.3.21051, a user could see boards without having corresponding permissions.	2021-08-06	4	CVE-2021-37554 MISC
jetbrains -- youtrack	In JetBrains YouTrack before 2021.2.16363, an insecure PRNG was used.	2021-08-06	5	CVE-2021-37553 MISC
jetbrains -- youtrack	In JetBrains YouTrack before 2021.2.16363, system user passwords were hashed with SHA-256.	2021-08-06	5	CVE-2021-37551 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetbrains -- youtrack	In JetBrains YouTrack before 2021.2.16363, time-unsafe comparisons were used.	2021-08-06	5	CVE-2021-37550 MISC
jetbrains -- youtrack	In JetBrains YouTrack before 2021.1.11111, sandboxing in workflows was insufficient.	2021-08-06	6.4	CVE-2021-37549 MISC
leostream -- connection_broker	** UNSUPPORTED WHEN ASSIGNED ** LeoStream Connection Broker 9.x before 9.0.34.3 allows Unauthenticated Reflected XSS via the /index.pl user parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-08-06	4.3	CVE-2021-38157 MISC MISC MISC MISC
linux -- linux_kernel	fs/nfsd/trace.h in the Linux kernel before 5.13.4 might allow remote attackers to cause a denial of service (out-of-bounds read in strlen) by sending NFS traffic when the trace event framework is being used for nfsd.	2021-08-08	5	CVE-2021-38202 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	In kernel/bpf/hashtab.c in the Linux kernel through 5.13.8, there is an integer overflow and out-of-bounds write when many elements are placed in a single bucket. NOTE: exploitation might be impractical without the CAP_SYS_ADMIN capability.	2021-08-07	4.6	CVE-2021-38166 MISC MISC
linux -- linux_kernel	fs/nfs/nfs4client.c in the Linux kernel before 5.13.4 has incorrect connection-setup ordering, which allows operators of remote NFSv4 servers to cause a denial of service (hanging of mounts) by arranging for those servers to be unreachable during trunking detection.	2021-08-08	5	CVE-2021-38199 MISC MISC
linux -- linux_kernel	net/sunrpc/xdr.c in the Linux kernel before 5.13.4 allows remote attackers to cause a denial of service (xdr_set_page_base slab-out-of-bounds access) by performing many NFS 4.2 READ_PLUS operations.	2021-08-08	5	CVE-2021-38201 MISC MISC
linux -- linux_kernel	drivers/net/ethernet/xilinx/ll_temac_main.c in the Linux kernel before 5.12.13 allows remote attackers to cause a denial of service (buffer	2021-08-08	5	CVE-2021-38207

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	overflow and lockup) by sending heavy network traffic for about ten minutes.			MISC MISC
lynx_project -- lynx	Lynx through 2.8.9 mishandles the userinfo subcomponent of a URI, which allows remote attackers to discover cleartext credentials because they may appear in SNI data.	2021-08-07	5	CVE-2021-38165 MISC MISC MISC MISC MISC MISC MLIST MLIST MLIST MLIST DEBIAN
naviwebs -- navigate_cms	SQL Injection vulnerability in Naviwebs Navigate CMS 2.9 via the quicksearch parameter in \lib\packages\comments\comments.php.	2021-08-06	6.5	CVE-2021-36455 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netapp -- cloud_manager	NetApp Cloud Manager versions prior to 3.9.9 log sensitive information when an Active Directory connection fails. The logged information is available only to authenticated users. Customers with auto-upgrade enabled should already be on a fixed version while customers using on-prem connectors with auto-upgrade disabled are advised to upgrade to a fixed version.	2021-08-06	4	CVE-2021-26999 MISC
netapp -- cloud_manager	NetApp Cloud Manager versions prior to 3.9.9 log sensitive information that is available only to authenticated users. Customers with auto-upgrade enabled should already be on a fixed version while customers using on-prem connectors with auto-upgrade disabled are advised to upgrade to a fixed version.	2021-08-06	4	CVE-2021-26998 MISC
popojicms -- popojicms	A stored cross site scripting (XSS) vulnerability in /admin.php?mod=user&act=addnew of PopojiCMS 1.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the E-Mail field.	2021-08-06	4.3	CVE-2020-21357 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
popojicms -- popojicms	An information disclosure vulnerability in upload.php of PopojiCMS 1.2 leads to physical path disclosure of the host when 'name = "file" is deleted during file uploads.	2021-08-06	5	CVE-2020-21356 MISC
project -- convec	An issue was discovered in the convec crate through 2020-11-24 for Rust. There are unconditional implementations of Send and Sync for ConVec<T>.	2021-08-08	6.8	CVE-2020-36445 MISC MISC
prolink -- prc2402m_firmware	In ProLink PRC2402M V1.0.18 and older, the set_sys_init function in the login.cgi binary allows an attacker to reset the password to the administrative interface of the router.	2021-08-06	5	CVE-2021-36708 MISC
qt -- qt	An issue has been fixed in Qt versions 5.14.1 and 5.12.7 where QLibrary attempts to load plugins relative to the working directory, allowing attackers to execute arbitrary code via crafted files.	2021-08-09	6.8	CVE-2020-24741 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qt -- qt	An issue has been fixed in Qt versions 5.14.0 where QPluginLoader attempts to load plugins relative to the working directory, allowing attackers to execute arbitrary code via crafted files.	2021-08-09	6.8	CVE-2020-24742 MISC
rconfig -- rconfig	The userLogin parameter in ldap/login.php of rConfig 3.9.5 is unsanitized, allowing attackers to perform a LDAP injection and obtain sensitive information via a crafted POST request.	2021-08-09	5	CVE-2020-23148 MISC
rconfig -- rconfig	The dbName parameter in ajaxDbInstall.php of rConfig 3.9.5 is unsanitized, allowing attackers to perform a SQL injection and access sensitive database information.	2021-08-09	5	CVE-2020-23149 MISC
rconfig -- rconfig	A SQL injection vulnerability in config.inc.php of rConfig 3.9.5 allows attackers to access sensitive database information via a crafted GET request to install/lib/ajaxHandlers/ajaxDbInstall.php.	2021-08-09	5	CVE-2020-23150 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
roxy-wi -- roxy-wi	Roxy-WI through 5.2.2.0 allows command injection via /app/funct.py and /api/api_funct.py.	2021-08-07	6.5	CVE-2021-38169 MISC
roxy-wi -- roxy-wi	Roxy-WI through 5.2.2.0 allows authenticated SQL injection via select_servers.	2021-08-07	6.5	CVE-2021-38168 MISC
ruspiro-singleton_project -- ruspiro-singleton	An issue was discovered in the ruspiro-singleton crate before 0.4.1 for Rust. In Singleton, Send and Sync do not have bounds checks.	2021-08-08	6.8	CVE-2020-36435 MISC MISC
sap -- businessobjects_edge	The File Repository Server (FRS) CORBA listener in SAP BussinessObjects Edge 4.0 allows remote attackers to write to arbitrary files via a full pathname, aka SAP Note 2018681.	2021-08-09	5	CVE-2015-2074 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- businessobjects_edge	The File RepositoRy Server (FRS) CORBA listener in SAP BussinessObjects Edge 4.0 allows remote attackers to read arbitrary files via a full pathname, aka SAP Note 2018682.	2021-08-09	5	CVE-2015-2073 MISC MISC MISC MISC
sap -- j2ee_engine	** UNSUPPORTED WHEN ASSIGNED ** A cross-site scripting (XSS) vulnerability in SAP J2EE Engine/7.01/Portal/EPP allows remote attackers to inject arbitrary web script via the wsdlLib parameter to /ctcprotocol/Protocol. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-08-09	4.3	CVE-2018-17861 BUGTRAQ FULLDISC MISC
sap -- j2ee_engine	** UNSUPPORTED WHEN ASSIGNED ** A cross-site scripting (XSS) vulnerability in SAP J2EE Engine/7.01/Fiori allows remote attackers to inject arbitrary web script via the sys_jdbc parameter to /TestJDBC_Web/test2. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-08-09	4.3	CVE-2018-17862 BUGTRAQ MISC FULLDISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- j2ee_engine	** UNSUPPORTED WHEN ASSIGNED ** A cross-site scripting (XSS) vulnerability in SAP J2EE Engine 7.01 allows remote attackers to inject arbitrary web script via the wsdlPath parameter to /ctcprotocol/Protocol. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-08-09	4.3	CVE-2018-17865 MISC
sapphireims -- sapphireims	In SapphireIMS 4097_1, it is possible to guess the registered/active usernames of the software from the errors it gives out for each type of user on the Login form. For "Incorrect User" - it gives an error "The application failed to identify the user. Please contact administrator for help." For "Correct User and Incorrect Password" - it gives an error "Authentication failed. Please login again."	2021-08-11	5	CVE-2017-16629 MISC MISC
signal-simple_project -- signal-simple	An issue was discovered in the signal-simple crate through 2020-11-15 for Rust. There are unconditional implementations of Send and Sync for SyncChannel<T>.	2021-08-08	6.8	CVE-2020-36446 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
southsoft -- graduate_management_information_system	Southsoft GMIS 5.0 is vulnerable to CSRF attacks. Attackers can access other users' private information such as photos through CSRF. For example: any student's photo information can be accessed through /gmis/(S([1]))/student/grgl/PotoImageShow/?bh=[2]. Among them, the code in [1] is a random string generated according to the user's login related information. It can protect the user's identity, but it can not effectively prevent unauthorized access. The code in [2] is the student number of any student. The attacker can carry out CSRF attack on the system by modifying [2] without modifying [1].	2021-08-06	6.8	CVE-2021-37381 MISC MISC
trendnet -- tew-755ap_firmware	Null Pointer Dereference vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service by sending the POST request to apply_cgi via the lang action without a language key.	2021-08-10	5	CVE-2021-28845 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wagecms_project -- wage-cms	A cross site request forgery (CSRF) in Wage-CMS 1.5.x-dev allows attackers to arbitrarily add users.	2021-08-06	4.3	CVE-2020-21358 MISC
yunucms -- yunucms	Cross Site Scripting (XSS) vulnerability exists in YUNUCMS 1.1.9 via the upurl function in Page.php.	2021-08-12	4.3	CVE-2020-18445 MISC MISC