Vulnerability Summary for the Week of February 1, 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
accel-ppp -- accel-ppp	Variable underflow exists in accel-ppp radius/packet.c when receiving a RADIUS vendor-specific attribute with length field is less than 2. It has an impact only when the attacker controls the RADIUS server, which can lead to arbitrary code execution.	2021-02-01	7.5	CVE-2020-28194 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adt -- lifeshield_diy_hd_video_doorbell_firmware	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in HTTP interface of ADT LifeShield DIY HD Video Doorbell allows an attacker on the same network to execute commands on the device. This issue affects: ADT LifeShield DIY HD Video Doorbell version 1.0.02R09 and prior versions.	2021-02-02	8.3	CVE-2020-8101 CONFIRM
apache -- druid	Apache Druid includes the ability to execute user-provided JavaScript code embedded in various types of requests. This functionality is intended for use in high-trust environments, and is disabled by default. However, in Druid 0.20.0 and earlier, it is possible for an authenticated user to send a specially-crafted request that forces Druid to run user-provided JavaScript code for that request, regardless of server configuration. This can be leveraged to execute code on the target machine with the privileges of the Druid server process.	2021-01-29	9	CVE-2021-25646 MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MISC MLIST

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
apache -- shiro	Apache Shiro before 1.7.1, when using Apache Shiro with Spring, a specially crafted HTTP request may cause an authentication bypass.	2021-02-03	9	CVE-2020-17523 MISC
asus -- rt-ax86u_firmware	ASUS RT-AX86U router firmware below version under 9.0.0.4_386 has a buffer overflow in the blocking_request.cgi function of the httpd module that can cause code execution when an attacker constructs malicious data.	2021-02-01	7.5	CVE-2020-36109 MISC
belkin -- linksys_wrt160nl_firmware	** UNSUPPORTED WHEN ASSIGNED ** The administration web interface on Belkin Linksys WRT160NL 1.0.04.002_US_20130619 devices allows remote authenticated attackers to execute system commands with root privileges via shell metacharacters in the ui_language POST parameter to the apply.cgi form endpoint. This occurs in do_upgrade_post in mini_httpd. NOTE: This vulnerability only affects products	2021-02-02	9	CVE-2021-25310 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	that are no longer supported by the maintainer			
bitovi -- launchpad	All versions of package launchpad are vulnerable to Command Injection via stop.	2021-02-01	7.5	CVE-2021-23330 CONFIRM CONFIRM CONFIRM
cdr_project -- cdr	An issue was discovered in Deserializer::read_vec in the cdr crate before 0.2.4 for Rust. A user-provided Read implementation can gain access to the old contents of newly allocated heap memory, violating soundness.	2021-01-29	7.5	CVE-2021-26305 MISC
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated,	2021-02-04	9	CVE-2021-1341 CISCO

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.			
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to	2021-02-04	9	CVE-2021-1337 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.			
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper	2021-02-04	9	CVE-2021-1338 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.			
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An	2021-02-04	9	CVE-2021-1339 CISCO

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.			
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP	2021-02-04	9	CVE-2021-1340 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.			
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the	2021-02-04	9	CVE-2021-1347 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.			
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating	2021-02-04	9	CVE-2021-1343 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.			
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS)	2021-02-04	9	CVE-2021-1344 CISCO

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.			
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need	2021-02-04	9	CVE-2021-1345 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to have valid administrator credentials on the affected device.			
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1346 CISCO

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1335 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1348 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1336 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1342 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1334 CISCO

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1324 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1333 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1319 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1320 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1321 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1322 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1323 CISCO

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1325 CISCO

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1326 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1327 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1328 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1329 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1330 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1331 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- rv016_multi-wan_vpn_router_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests 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 denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	2021-02-04	9	CVE-2021-1332 CISCO
cmswing -- cmswing	An issue was found in CMSWing project version 1.3.8. Because the log	2021-02-01	7.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	function does not check the log parameter, malicious parameters can execute arbitrary commands.			20294 MISC
cmswing -- cmswing	An issue was found in CMSWing project version 1.3.8, Because the rechargeAction function does not check the balance parameter, malicious parameters can execute arbitrary SQL commands.	2021-02-01	7.5	CVE-2020-20296 MISC
cmswing -- cmswing	An issue was found in CMSWing project version 1.3.8. Because the updateAction function does not check the detail parameter, malicious parameters can execute arbitrary SQL commands.	2021-02-01	7.5	CVE-2020-20295 MISC
dlink -- dns-320_firmware	D-Link DNS-320 FW v2.06B01 Revision Ax is affected by command injection in the system_mgr.cgi component, which can lead to remote arbitrary code execution.	2021-02-02	7.5	CVE-2020-25506 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dlink -- dsr-250_firmware	The D-Link DSR-250 (3.14) DSR-1000N (2.11B201) UPnP service contains a command injection vulnerability, which can cause remote command execution.	2021-02-02	7.5	CVE-2020-18568 MISC MISC
dotty_project -- dotty	Prototype pollution vulnerability in 'dotty' versions 0.0.1 through 0.1.0 allows attackers to cause a denial of service and may lead to remote code execution.	2021-02-02	7.5	CVE-2021-25912 MISC MISC
fortilogger -- fortilogger	FortiLogger 4.4.2.2 is affected by Arbitrary File Upload by sending a "Content-Type: image/png" header to Config/SaveUploadedHotspotLogoFile and then visiting Assets/temp/hotspot/img/logohotspot.asp.	2021-02-01	7.5	CVE-2021-3378 MISC
gnupg -- libgcrypt	_gcry_md_block_write in cipher/hash-common.c in Libgcrypt version 1.9.0 has a heap-based buffer overflow when the digest final function sets a large	2021-01-29	7.2	CVE-2021-3345 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	count value. It is recommended to upgrade to 1.9.1 or later.			MISC MISC
google -- android	In kisd, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05449962.	2021-02-04	7.2	CVE-2021-0343 MISC
google -- android	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10 software. The USB laf gadget has a use-after-free. The LG ID is LVE-SMP-200031 (February 2021).	2021-02-04	7.5	CVE-2021-26689 MISC
google -- android	In vpu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product:	2021-02-04	7.2	CVE-2021-0348 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Android; Versions: Android-11; Patch ID: ALPS05349201.			
google -- android	In display driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05362646.	2021-02-04	7.2	CVE-2021-0349 MISC
google -- android	In mtkpower, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05437558.	2021-02-04	7.2	CVE-2021-0344 MISC
google -- android	In wlan driver, there is a possible system crash due to a missing bounds check. This could lead to remote denial	2021-02-04	7.8	CVE-2021-0351 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05412917.			
google -- android	In vpu, 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. Product: Android; Versions: Android-11; Patch ID: ALPS05371580.	2021-02-04	7.2	CVE-2021-0346 MISC
google -- android	In mobile_log_d, there is a possible escalation of privilege 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. Product: Android; Versions: Android-11; Patch ID: ALPS05432974.	2021-02-04	7.2	CVE-2021-0345 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA before 2020.3, potentially insecure deserialization of the workspace model could lead to code execution.	2021-02-03	7.5	CVE-2021-25758 MISC MISC
jetbrains -- youtrack	In JetBrains YouTrack before 2020.5.3123, server-side template injection (SSTI) was possible, which could lead to code execution.	2021-02-03	7.5	CVE-2021-25770 MISC MISC
kill-process-on-port_project -- kill-process-on-port	All versions of package kill-process-on-port are vulnerable to Command Injection via a.getProcessPortId.	2021-02-01	7.5	CVE-2020-28426 MISC
koa2-blog_project -- koa2-blog	Sql injection vulnerability in koa2-blog 1.0.0 allows remote attackers to Injecting a malicious SQL statement via the name parameter to the signin page.	2021-02-01	7.5	CVE-2020-21179 MISC
koa2-blog_project -- koa2-blog	Sql injection vulnerability in koa2-blog 1.0.0 allows remote attackers to	2021-02-01	7.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Injecting a malicious SQL statement via the name parameter to the signup page.			21180 MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.	2021-01-29	7.2	CVE-2021-3347 MLIST MLIST MLIST MISC MISC MISC MISC MISC MISC MISC MISC FEDORA FEDORA DEBIAN MISC MISC
mofinetwork -- mofi4500-4gxelte_firmware	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.1.5-std devices. The Dropbear SSH daemon has been modified to accept an alternate	2021-02-01	10	CVE-2020-15833

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	hard-coded path to a public key that allows root access. This key is stored in a /rom location that cannot be modified by the device owner.			MISC MISC
mofinetwork -- mofi4500-4gxelte_firmware	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 3.6.1-std and 4.0.8-std devices. They contain two undocumented administrator accounts. The sftp and mofidev accounts are defined in /etc/passwd and the password is not unique across installations.	2021-02-01	7.5	CVE-2020-13858 MISC MISC
mofinetwork -- mofi4500-4gxelte_firmware	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.1.5-std devices. The authentication function contains undocumented code that provides the ability to authenticate as root without knowing the actual root password. An adversary with the private key can remotely authenticate to the management interface as root.	2021-02-01	10	CVE-2020-15835 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mofinetwork -- mofi4500-4gxelte_firmware	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.1.5-std devices. The authentication function passes untrusted data to the operating system without proper sanitization. A crafted request can be sent to execute arbitrary commands as root.	2021-02-01	10	CVE-2020-15836 MISC MISC
mofinetwork -- mofi4500-4gxelte_firmware	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 3.6.1-std and 4.0.8-std devices. They can be rebooted by sending an unauthenticated poof.cgi HTTP GET request.	2021-02-01	7.8	CVE-2020-13857 MISC MISC
mofinetwork -- mofi4500-4gxelte_firmware	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.1.5-std devices. The poof.cgi script contains undocumented code that provides the ability to remotely reboot the device. An adversary with the private key (but not the root password) can remotely reboot the device.	2021-02-01	7.8	CVE-2020-15832 MISC MISC
moxa -- edr-g903_firmware	Certain Moxa Inc products are affected by an improper restriction of operations	2021-02-03	7.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in EDR-G903 Series Firmware Version 5.5 or lower, EDR-G902 Series Firmware Version 5.5 or lower, and EDR-810 Series Firmware Version 5.6 or lower. Crafted requests sent to the device may allow remote arbitrary code execution.			28144 MISC
nic -- foris	Foris before 101.1.1, as used in Turris OS, lacks certain HTML escaping in the login template.	2021-01-29	7.5	CVE-2021-3346 MISC MISC MISC
nim-lang -- nim	In Nim before 1.2.6, the standard library asyncftpclient lacks a check for whether a message contains a newline character.	2021-01-30	7.5	CVE-2020-15690 MLIST MISC MISC CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qnap -- helpdesk	The vulnerability have been reported to affect earlier versions of QTS. If exploited, this improper access control vulnerability could allow attackers to obtain control of a QNAP device. This issue affects: QNAP Systems Inc. Helpdesk versions prior to 3.0.3.	2021-02-03	7.5	CVE-2020-2506 CONFIRM
qnap -- helpdesk	The vulnerability have been reported to affect earlier versions of QTS. If exploited, this improper access control vulnerability could allow attackers to obtain control of a QNAP device. This issue affects: QNAP Systems Inc. Helpdesk versions prior to 3.0.3.	2021-02-03	7.5	CVE-2020-2507 CONFIRM
rainbowfishsoftware -- pacsone_server	PacsOne Server (PACS Server In One Box) below 7.1.1 is affected by incorrect access control, which can result in remotely gaining administrator privileges.	2021-02-03	7.5	CVE-2020-29165 MISC MISC
rockoa -- rockoa	SQL Injection in Rockoa v1.8.7 allows remote attackers to gain privileges due	2021-02-05	7.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to loose filtering of parameters in wordAction.php.			18716 MISC
rockoa -- rockoa	SQL Injection in Rockoa v1.8.7 allows remote attackers to gain privileges due to loose filtering of parameters in wordModel.php's getdata function.	2021-02-05	7.5	CVE-2020-18714 MISC
rockoa -- rockoa	SQL Injection in Rockoa v1.8.7 allows remote attackers to gain privileges due to loose filtering of parameters in customerAction.php	2021-02-05	7.5	CVE-2020-18713 MISC
solarwinds -- serv-u	SolarWinds Serv-U before 15.2.2 allows Unauthenticated Macro Injection.	2021-02-03	7.5	CVE-2020-35481 CONFIRM
terra-master -- tos	TerraMaster TOS before 4.1.29 has Invalid Parameter Checking that leads to code injection as root. This is a dynamic class method invocation vulnerability in include/exportUser.php, in which an	2021-01-30	10	CVE-2020-15568 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker can trigger a call to the exec method with (for example) OS commands in the opt parameter.			
thinkjs -- thinkjs	SQL injection vulnerability in the model.increment and model.decrement function in ThinkJS 3.2.10 allows remote attackers to execute arbitrary SQL commands via the step parameter.	2021-02-01	7.5	CVE-2020-21176 MISC MISC
tk-star -- q90_junior_gps_horloge_firmware	An issue was discovered in SeTracker2 for TK-Star Q90 Junior GPS horloge 3.1042.9.8656 devices. It has unnecessary permissions such as READ_EXTERNAL_STORAGE, WRITE_EXTERNAL_STORAGE, and READ_CONTACTS.	2021-02-01	7.5	CVE-2019-20468 MISC MISC
tk-star -- q90_junior_gps_horloge_firmware	An issue was discovered on TK-Star Q90 Junior GPS horloge 3.1042.9.8656 devices. When using the device at initial setup, a default password is used (123456) for administrative purposes. There is no prompt to change this password. Note that this password can	2021-02-01	7.2	CVE-2019-20471 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	be used in combination with CVE-2019-20470.			
totaljs -- total.js	This affects the package total.js before 3.4.7. The set function can be used to set a value into the object according to the path. However the keys of the path being set are not properly sanitized, leading to a prototype pollution vulnerability. The impact depends on the application. In some cases it is possible to achieve Denial of service (DoS), Remote Code Execution or Property Injection.	2021-02-02	7.5	CVE-2020-28495 MISC MISC MISC MISC MISC
totaljs -- total.js	This affects the package total.js before 3.4.7. The issue occurs in the image.pipe and image.stream functions. The type parameter is used to build the command that is then executed using child_process.spawn. The issue occurs because child_process.spawn is called with the option shell set to true and because the type parameter is not properly sanitized.	2021-02-02	7.5	CVE-2020-28494 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
trendmicro -- apex_one	An out-of-bounds write information disclosure vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security (10.0 SP1 and Services) could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2021-02-04	7.2	CVE-2021-25249 N/A N/A N/A N/A
ucopia -- express_wireless_appliance	UCOPIA Wi-Fi appliances 6.0.5 allow arbitrary code execution with root privileges using chroothole_client's PHP call, a related issue to CVE-2017-11322.	2021-02-02	7.2	CVE-2020-25035 MISC MISC
ucopia -- ucopia_wireless_appliance	UCOPIA Wi-Fi appliances 6.0.5 allow arbitrary code execution with admin user privileges via an escape from a restricted command.	2021-02-02	7.2	CVE-2020-25037 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ucopia -- ucopia_wireless_appliance	UCOPIA Wi-Fi appliances 6.0.5 allow authenticated remote attackers to escape the restricted administration shell CLI, and access a shell with admin user rights, via an unprotected less command.	2021-02-02	9	CVE-2020-25036 MISC MISC
windriver -- vxworks	In Wind River VxWorks, memory allocator has a possible overflow in calculating the memory block's size to be allocated by calloc(). As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.	2021-02-03	7.5	CVE-2020-28895 MISC MISC
wolfssl -- wolfssl	DoTls13CertificateVerify in tls13.c in wolfSSL through 4.6.0 does not cease processing for certain anomalous peer behavior (sending an ED22519, ED448, ECC, or RSA signature without the corresponding certificate).	2021-01-29	7.5	CVE-2021-3336 MISC
yccms -- yccms	Unrestricted file upload vulnerability in the yccms 3.3 project. The xhUp	2021-02-01	7.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	function's improper judgment of the request parameters, triggers remote code execution.			20287 MISC MISC
yccms -- yccms	Sql injection vulnerability in the yccms 3.3 project. The no_top function's improper judgment of the request parameters, triggers a sql injection vulnerability.	2021-02-01	7.5	CVE-2020-20289 MISC MISC
zohocorp -- manageengine_opmanager	Zoho ManageEngine OpManager Stable build before 125203 (and Released build before 125233) allows Remote Code Execution via the Smart Update Manager (SUM) servlet.	2021-02-03	7.5	CVE-2020-28653 CONFIRM CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acronis -- true_image	Acronis True Image for Windows prior to 2021 Update 3 allowed local privilege escalation due to a DLL hijacking vulnerability in multiple components, aka an Untrusted Search Path issue.	2021-01-29	4.4	CVE-2020-35145 MISC CONFIRM
adobe -- adobe_consulting_services_commons	ACS Commons version 4.9.2 (and earlier) suffers from a Reflected Cross-site Scripting (XSS) vulnerability in version-compare and page-compare due to invalid JCR characters that are not handled correctly. An attacker could potentially exploit this vulnerability to inject malicious JavaScript content into vulnerable form fields and execute it within the context of the victim's browser. Exploitation of this issue requires user interaction in order to be successful.	2021-02-02	4.3	CVE-2021-21043 CONFIRM
apache -- cassandra	Apache Cassandra versions 2.1.0 to 2.1.22, 2.2.0 to 2.2.19, 3.0.0 to 3.0.23, and 3.11.0 to 3.11.9, when using 'dc' or 'rack' internode_encryption setting, allows both encrypted and unencrypted internode connections. A misconfigured node or a malicious user can use the unencrypted connection despite not being in the same rack or dc, and bypass mutual TLS requirement.	2021-02-03	4.3	CVE-2020-17516 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- crucible	Affected versions of Atlassian Fisheye and Crucible allow remote attackers to view a product's SEN via an Information Disclosure vulnerability in the x-asen response header from Atlassian Analytics. The affected versions are before version 4.8.4.	2021-02-02	4	CVE-2020-14192 MISC MISC
atlassian -- jira	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to view the metadata of boards they should not have access to via an Insecure Direct Object References (IDOR) vulnerability. The affected versions are before version 8.5.10, and from version 8.6.0 before 8.13.2.	2021-02-02	4	CVE-2020-36231 MISC
cisco -- advanced_malware_protection	A TOCTOU vulnerability exists in madCodeHook before 2020-07-16 that allows local attackers to elevate their privileges to SYSTEM. This occurs because path redirection can occur via vectors involving directory junctions.	2021-01-30	6.9	CVE-2020-14418 MISC MISC
ckeditor -- ckeditor_5	CKEditor 5 is an open source rich text editor framework with a modular architecture. The CKEditor 5 Markdown plugin (@ckeditor/ckeditor5-markdown-gfm) before version 25.0.0 has a regex denial of service (ReDoS) vulnerability. The vulnerability allowed to abuse link recognition regular expression, which could cause a significant performance drop	2021-01-29	4	CVE-2021-21254 MISC CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	resulting in browser tab freeze. It affects all users using CKEditor 5 Markdown plugin at version <= 24.0.0. The problem has been recognized and patched. The fix will be available in version 25.0.0.			RM MISC
cloudflare -- warp	Cloudflare WARP for Windows allows privilege escalation due to an unquoted service path. A malicious user or process running with non-administrative privileges can become an administrator by abusing the unquoted service path issue. Since version 1.2.2695.1, the vulnerability was fixed by adding quotes around the service's binary path. This issue affects Cloudflare WARP for Windows, versions prior to 1.2.2695.1.	2021-02-03	4.6	CVE-2020-35152 CONFIRM
delete_account_project -- delete_account	deleteaccount.php in the Delete Account plugin 1.4 for MyBB allows XSS via the deletereason parameter.	2021-02-01	4.3	CVE-2021-3350 MISC
dh2i -- dxenterprise	A path traversal vulnerability in the DxWebEngine component of DH2i DxEnterprise and DxOdyssey for Windows, version 19.5 through 20.x before 20.0.219.0, allows an attacker to read any file on the host file system via an HTTP request.	2021-01-29	5	CVE-2021-3341 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
digium -- asterisk	An issue was discovered in res_pjsip_diversion.c in Sangoma Asterisk before 13.38.0, 14.x through 16.x before 16.15.0, 17.x before 17.9.0, and 18.x before 18.1.0. A crash can occur when a SIP message is received with a History-Info header that contains a tel-uri, or when a SIP 181 response is received that contains a tel-uri in the Diversion header.	2021-01-29	4	CVE-2020-35652 CONFIRM CONFIRM MISC MISC
djangoproject -- django	In Django 2.2 before 2.2.18, 3.0 before 3.0.12, and 3.1 before 3.1.6, the django.utils.archive.extract method (used by "startapp --template" and "startproject --template") allows directory traversal via an archive with absolute paths or relative paths with dot segments.	2021-02-02	5	CVE-2021-3281 MISC MISC CONFIRM
easycms -- easycms	A CSRF vulnerability was discovered in EasyCMS v1.6 that can add an admin account through index.php?s=/admin/rbacuser/insert/navTabId/rbacuser/callbackType/closeCurrent, then post username=***&password=***.	2021-02-01	6.8	CVE-2020-24271 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
facebook -- hermes	A stack overflow vulnerability in Facebook Hermes â€˜builtin applyâ€™ prior to commit 86543ac47e59c522976b5632b8bf9a2a4583c7d2 (https://github.com/facebook/hermes/commit/86543ac47e59c522976b5632b8bf9a2a4583c7d2) allows attackers to potentially execute arbitrary code via crafted JavaScript. Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications are not affected.	2021-02-02	6.8	CVE-2020-1896 CONFIRM CONFIRM
getadigital -- nested-object-assign	The package nested-object-assign before 1.0.4 are vulnerable to Prototype Pollution via the default function, as demonstrated by running the PoC below.	2021-01-31	5	CVE-2021-23329 MISC MISC
google -- android	In netdiag, 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. Product: Android; Versions: Android-11; Patch ID: ALPS05442006.	2021-02-03	4.6	CVE-2021-0360 MISC
google -- android	In netdiag, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege	2021-02-03	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05442022.			0358 MISC
google -- android	In netdiag, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05442011.	2021-02-03	4.6	CVE-2021-0359 MISC
google -- android	In ged, there is a possible out of bounds write 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. Product: Android; Versions: Android-11; Patch ID: ALPS05431161.	2021-02-03	4.6	CVE-2021-0354 MISC
google -- android	In netdiag, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05442002.	2021-02-03	4.6	CVE-2021-0357 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In netdiag, there is a possible command injection 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. Product: Android; Versions: Android-11; Patch ID: ALPS05442014.	2021-02-03	4.6	CVE-2021-0356 MISC
google -- android	In kisd, there is a possible out of bounds write 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. Product: Android; Versions: Android-11; Patch ID: ALPS05425581.	2021-02-03	4.6	CVE-2021-0355 MISC
google -- android	In kisd, there is a possible memory corruption due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05425247.	2021-02-03	4.6	CVE-2021-0353 MISC
google -- android	In ged, there is a possible system crash due to an improper input validation. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05342338.	2021-02-04	4.9	CVE-2021-0350 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In kisd, there is a possible out of bounds read 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. Product: Android; Versions: Android-11; Patch ID: ALPS05449968.	2021-02-03	4.6	CVE-2021-0361 MISC
google -- android	In aee, there is a possible memory corruption due to a stack buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05457070.	2021-02-03	4.6	CVE-2021-0362 MISC
google -- android	In mobile_log_d, there is a possible command injection due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05458478.	2021-02-03	4.6	CVE-2021-0363 MISC
google -- android	In mobile_log_d, there is a possible command injection 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. Product: Android; Versions: Android-11; Patch ID: ALPS05458478; Issue ID: ALPS05458503.	2021-02-03	4.6	CVE-2021-0364 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In display driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05454782.	2021-02-03	4.6	CVE-2021-0365 MISC
hashicorp -- nomad	HashiCorp Nomad and Nomad Enterprise up to 0.12.9 exec and java task drivers can access processes associated with other tasks on the same node. Fixed in 0.12.10, and 1.0.3.	2021-02-01	5	CVE-2021-3283 MISC
hashicorp -- vault	HashiCorp Vault and Vault Enterprise allowed for enumeration of Secrets Engine mount paths via unauthenticated HTTP requests. Fixed in 1.6.2 & 1.5.7.	2021-02-01	5	CVE-2020-25594 MISC
hashicorp -- vault	HashiCorp Vault and Vault Enterprise disclosed the internal IP address of the Vault node when responding to some invalid, unauthenticated HTTP requests. Fixed in 1.6.2 & 1.5.7.	2021-02-01	5	CVE-2021-3024 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hashicorp -- vault	HashiCorp Vault Enterprise 1.6.0 & 1.6.1 allowed the `remove-peer` raft operator command to be executed against DR secondaries without authentication. Fixed in 1.6.2.	2021-02-01	5	CVE-2021-3282 MISC
hcltechsw -- onetest_performance	HCL OneTest Performance V9.5, V10.0, V10.1 contains an inadequate session timeout, which could allow an attacker time to guess and use a valid session ID.	2021-02-04	6.4	CVE-2020-14247 MISC
hcltechsw -- onetest_performance	HCL OneTest Performance V9.5, V10.0, V10.1 uses basic authentication which is relatively weak. An attacker could potentially decode the encoded credentials.	2021-02-04	5	CVE-2020-14246 MISC
hitachi -- vantara_pentaho	The Dashboard Editor in Hitachi Vantara Pentaho through 7.x - 8.x contains an XML Entity Expansion injection vulnerability, which allows an authenticated remote users to trigger a denial of service (DoS) condition. Specifically, the vulnerability lies in the 'dashboardXml' parameter. Remediated in >= 7.1.0.25, >= 8.2.0.6, >= 8.3.0.0 GA	2021-01-29	4	CVE-2020-24665 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- api_connect	IBM API Connect 10.0.0.0 through 10.0.1.0 and 2018.4.1.0 through 2018.4.1.13 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: 189840.	2021-02-04	4.3	CVE-2020-4826 XF CONFIRM
ibm -- api_connect	IBM API Connect 10.0.0.0 through 10.0.1.0 and 2018.4.1.0 through 2018.4.1.13 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: 189841.	2021-02-04	4.3	CVE-2020-4827 XF CONFIRM
ibm -- api_connect	IBM API Connect 10.0.0.0 through 10.0.1.0 and 2018.4.1.0 through 2018.4.1.13 is vulnerable to web cache poisoning, caused by improper input validation by modifying HTTP request headers. IBM X-Force ID: 189842.	2021-02-04	6.4	CVE-2020-4828 XF CONFIRM
ibm -- content_navigator	IBM Content Navigator 3.0.CD could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences	2021-02-02	4	CVE-2020-4934

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(/../) to view arbitrary files on the system. IBM X-Force ID: 191752.			XF CONFIRM
iniparserjs_project -- iniparserjs	This affects all versions of package iniparserjs. This vulnerability relates when ini_parser.js is concentrating arrays. Depending on if user input is provided, an attacker can overwrite and pollute the object prototype of a program.	2021-01-29	6.8	CVE-2021-23328 MISC MISC
intel -- m10jnp2sb_firmware	Improper input validation in the firmware for Intel(R) Server Board M10JNP2SB before version 7.210 may allow a privileged user to potentially enable escalation of privilege via local access.	2021-02-02	4.6	CVE-2020-8734 CONFIRM
iris -- star	A Cross-Site Request Forgery (CSRF) vulnerability exists in Star Practice Management Web version 2019.2.0.6, allowing an attacker to change the privileges of any user of the application. This can be used to grant himself administrative role or remove the administrative account of the application.	2021-01-29	6.8	CVE-2020-28403 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
istio -- istio	A NULL pointer dereference was found in pkg/proxy/envoy/v2/debug.go getResourceVersion in Istio pilot before 1.5.0-alpha.0. If a particular HTTP GET request is made to the pilot API endpoint, it is possible to cause the Go runtime to panic (resulting in a denial of service to the istio-pilot application).	2021-01-29	4	CVE-2019-25014 MISC MISC
jetbrains -- hub	In JetBrains Hub before 2020.1.12629, an open redirect was possible.	2021-02-03	5.8	CVE-2021-25757 MISC MISC
jetbrains -- hub	In JetBrains Hub before 2020.1.12669, information disclosure via the public API was possible.	2021-02-03	5	CVE-2021-25760 MISC MISC
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA before 2020.2, HTTP links were used for several remote repositories instead of HTTPS.	2021-02-03	5	CVE-2021-25756 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetbrains -- kotlin	In JetBrains Kotlin before 1.4.21, a vulnerable Java API was used for temporary file and folder creation. An attacker was able to read data from such files and list directories due to insecure permissions.	2021-02-03	5	CVE-2020-29582 MISC MISC
jetbrains -- ktor	In JetBrains Ktor before 1.4.2, weak cipher suites were enabled by default.	2021-02-03	5	CVE-2021-25763 MISC MISC
jetbrains -- teamcity	JetBrains TeamCity before 2020.2 was vulnerable to reflected XSS on several pages.	2021-02-03	4.3	CVE-2021-25773 MISC MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.1, permissions during user deletion were checked improperly.	2021-02-03	5	CVE-2021-25778 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.1, permissions during token removal were checked improperly.	2021-02-03	5	CVE-2021-25777 MISC MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2, an ECR token could be exposed in a build's parameters.	2021-02-03	5	CVE-2021-25776 MISC MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.2, TeamCity server DoS was possible via server integration.	2021-02-03	5	CVE-2021-25772 MISC MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.1, a user could get access to the GitHub access token of another user.	2021-02-03	4	CVE-2021-25774 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetbrains -- teamcity	JetBrains TeamCity Plugin before 2020.2.85695 SSRF. Vulnerability that could potentially expose user credentials.	2021-02-03	5	CVE-2020-35667 MISC MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.1, the server admin could create and see access tokens for any other users.	2021-02-03	5.5	CVE-2021-25775 MISC MISC
jetbrains -- youtrack	In JetBrains YouTrack before 2020.4.4701, CSRF via attachment upload was possible.	2021-02-03	6.8	CVE-2021-25765 MISC MISC
jetbrains -- youtrack	In JetBrains YouTrack before 2020.4.6808, the YouTrack administrator wasn't able to access attachments.	2021-02-03	5	CVE-2021-25769 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetbrains -- youtrack	In JetBrains YouTrack before 2020.4.4701, permissions for attachments actions were checked improperly.	2021-02-03	5	CVE-2021-25768 MISC MISC
jetbrains -- youtrack	In JetBrains YouTrack before 2020.4.4701, an attacker could enumerate users via the REST API without appropriate permissions.	2021-02-03	5	CVE-2020-25208 MISC MISC
jetbrains -- youtrack	In JetBrains YouTrack before 2020.6.1099, project information could be potentially disclosed.	2021-02-03	5	CVE-2021-25771 MISC MISC
jetbrains -- youtrack	In JetBrains YouTrack before 2020.6.1767, an issue's existence could be disclosed via YouTrack command execution.	2021-02-03	5	CVE-2021-25767 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
marc_project -- marc	An issue was discovered in the marc crate before 2.0.0 for Rust. A user-provided Read implementation can gain access to the old contents of newly allocated memory, violating soundness.	2021-01-29	5	CVE-2021-26308 MISC
mediawiki -- mediawiki	The API in the Push extension for MediaWiki through 1.35 used cleartext for ApiPush credentials, allowing for potential information disclosure.	2021-01-29	5	CVE-2020-29005 MISC MISC
mediawiki -- mediawiki	The API in the Push extension for MediaWiki through 1.35 did not require an edit token in ApiPushBase.php and therefore facilitated a CSRF attack.	2021-01-29	6.8	CVE-2020-29004 MISC CONFIRM MISC
minio -- minio	MinIO is a High Performance Object Storage released under Apache License v2.0. In MinIO before version RELEASE.2021-01-30T00-20-58Z there is a server-side request forgery vulnerability. The target application may have functionality for importing data from a URL, publishing data to a URL, or	2021-02-01	4	CVE-2021-21287 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	otherwise reading data from a URL that can be tampered with. The attacker modifies the calls to this functionality by supplying a completely different URL or by manipulating how URLs are built (path traversal etc.). In a Server-Side Request Forgery (SSRF) attack, the attacker can abuse functionality on the server to read or update internal resources. The attacker can supply or modify a URL which the code running on the server will read or submit data, and by carefully selecting the URLs, the attacker may be able to read server configuration such as AWS metadata, connect to internal services like HTTP enabled databases, or perform post requests towards internal services which are not intended to be exposed. This is fixed in version RELEASE.2021-01-30T00-20-58Z, all users are advised to upgrade. As a workaround you can disable the browser front-end with "MINIO_BROWSER=off" environment variable.			MISC CONFIRM
mit -- krb5-appl	An issue was discovered in rcp in MIT krb5-appl through 1.0.3. Due to the rcp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the rcp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious rcp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the rcp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the	2021-02-02	5.8	CVE-2019-25017 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	.ssh/authorized_keys file). This issue is similar to CVE-2019-6111 and CVE-2019-7283. NOTE: MIT krb5-appl is not supported upstream but is shipped by a few Linux distributions. The affected code was removed from the supported MIT Kerberos 5 (aka krb5) product many years ago, at version 1.8.			
mit -- krb5-appl	In the rcp client in MIT krb5-appl through 1.0.3, malicious servers could bypass intended access restrictions via the filename of . or an empty filename, similar to CVE-2018-20685 and CVE-2019-7282. The impact is modifying the permissions of the target directory on the client side. NOTE: MIT krb5-appl is not supported upstream but is shipped by a few Linux distributions. The affected code was removed from the supported MIT Kerberos 5 (aka krb5) product many years ago, at version 1.8.	2021-02-02	5	CVE-2019-25018 MISC
mitel -- businesscti_enterprise	The chat window of the Mitel BusinessCTI Enterprise (MBC-E) Client for Windows before 6.4.15 and 7.x before 7.1.2 could allow an attacker to gain access to user information by sending certain code, due to improper input validation of http links. A successful exploit could allow an attacker to view user information and application data.	2021-01-29	6	CVE-2021-3176 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mitel -- micollab	A library index page in NuPoint Messenger in Mitel MiCollab before 9.2 FP1 could allow an unauthenticated attacker to gain access (view and modify) to user data.	2021-01-29	6.4	CVE-2020-35547 MISC CONFIRM
mofinetwork -- mofi4500-4gxelte_firmware	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.0.8-std devices. Authentication is not required to download the support file that contains sensitive information such as cleartext credentials and password hashes.	2021-02-01	5	CVE-2020-13856 MISC MISC
mofinetwork -- mofi4500-4gxelte_firmware	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.0.8-std devices. A format error in /etc/shadow, coupled with a logic bug in the LuCI - OpenWrt Configuration Interface framework, allows the undocumented system account mofidev to login to the cgi-bin/luci/quick/wizard management interface without a password by abusing a forgotten-password feature.	2021-02-01	5	CVE-2020-13859 MISC MISC
mofinetwork -- mofi4500-4gxelte_firmware	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.1.5-std devices. The wireless network password is	2021-02-01	5	CVE-2020-15834

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exposed in a QR encoded picture that an unauthenticated adversary can download via the web-management interface.			MISC MISC
mofinetwork -- mofi4500-4gxelte_firmware	An issue was discovered on Mofi Network MOFI4500-4GXeLTE 4.0.8-std devices. The one-time password algorithm for the undocumented system account mofidev generates a predictable six-digit password.	2021-02-01	5	CVE-2020-13860 MISC MISC
monal -- monal	Monal before 4.9 does not implement proper sender verification on MAM and Message Carbon (XEP-0280) results. This allows a remote attacker (able to send stanzas to a victim) to inject arbitrary messages into the local history, with full control over the sender and receiver displayed to the victim.	2021-02-01	5	CVE-2020-26547 MISC CONFIRM
nagios -- favorites	The Favorites component before 1.0.2 for Nagios XI 5.8.0 is vulnerable to Insecure Direct Object Reference: it is possible to create favorites for any other user account.	2021-02-03	5	CVE-2021-26024 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nagios -- favorites	The Favorites component before 1.0.2 for Nagios XI 5.8.0 is vulnerable to XSS.	2021-02-03	4.3	CVE-2021-26023 CONFIRM
openhab -- openhab	openHAB is a vendor and technology agnostic open source automation software for your home. In openHAB before versions 2.5.12 and 3.0.1 the XML external entity (XXE) attack allows attackers in the same network as the openHAB instance to retrieve internal information like the content of files from the file system. Responses to SSDP requests can be especially malicious. All add-ons that use SAX or JAXB parsing of externally received XML are potentially subject to this kind of attack. In openHAB, the following add-ons are potentially impacted: AvmFritz, BoseSoundtouch, DenonMarantz, DLinkSmarthome, Enigma2, FmiWeather, FSInternetRadio, Gce, Homematic, HPPrinter, IHC, Insteon, Onkyo, Roku, SamsungTV, Sonos, Roku, Tellstick, TR064, UPnPControl, Vitotronic, Wemo, YamahaReceiver and XPath Tranformation. The vulnerabilities have been fixed in versions 2.5.12 and 3.0.1 by a more strict configuration of the used XML parser.	2021-02-01	4	CVE-2021-21266 MISC MISC CONFIRM MISC
palletsprojects -- jinja	This affects the package jinja2 from 0.0.0 and before 2.11.3. The ReDOS vulnerability of the regex is mainly due to the sub-	2021-02-01	5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	pattern [a-zA-Z0-9._-]+.[a-zA-Z0-9._-]+ This issue can be mitigated by Markdown to format user content instead of the urlize filter, or by implementing request timeouts and limiting process memory.			28493 MISC MISC MISC
phpgacl_project -- phpgacl	A cross-site scripting vulnerability exists in the template functionality of phpGACL 3.3.7. A specially crafted HTTP request can lead to arbitrary JavaScript execution. An attacker can provide a crafted URL to trigger this vulnaerability in the phpGACL template action parameter.	2021-02-01	4.3	CVE-2020-13562 MISC
phpgacl_project -- phpgacl	A cross-site scripting vulnerability exists in the template functionality of phpGACL 3.3.7. A specially crafted HTTP request can lead to arbitrary JavaScript execution. An attacker can provide a crafted URL to trigger this vulnerability in the phpGACL template acl_id parameter.	2021-02-01	4.3	CVE-2020-13564 MISC
phpgacl_project -- phpgacl	A cross-site scripting vulnerability exists in the template functionality of phpGACL 3.3.7. A specially crafted HTTP request can lead to arbitrary JavaScript execution. An attacker can provide a crafted URL to trigger this vulnerability in the phpGACL template group_id parameter.	2021-02-01	4.3	CVE-2020-13563 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qemu -- qemu	A heap-based buffer overflow was found in QEMU through 5.0.0 in the SDHCI device emulation support. It could occur while doing a multi block SDMA transfer via the sdhci_sdma_transfer_multi_blocks() routine in hw/sd/sdhci.c. A guest user or process could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition, or potentially execute arbitrary code with privileges of the QEMU process on the host.	2021-01-30	4.6	CVE-2020-17380 CONFIRM CONFIRM
rainbowfishsoftware -- pacsone_server	PacsOne Server (PACS Server In One Box) below 7.1.1 is affected by cross-site scripting (XSS).	2021-02-03	4.3	CVE-2020-29164 MISC MISC
rainbowfishsoftware -- pacsone_server	PacsOne Server (PACS Server In One Box) below 7.1.1 is affected by SQL injection.	2021-02-03	6.5	CVE-2020-29163 MISC MISC
rainbowfishsoftware -- pacsone_server	PacsOne Server (PACS Server In One Box) below 7.1.1 is affected by file read/manipulation, which can result in remote information disclosure.	2021-02-03	5	CVE-2020-29166

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
raw-cpuid_project -- raw-cpuid	An issue was discovered in the raw-cpuid crate before 9.0.0 for Rust. It has unsound transmute calls within as_string() methods.	2021-01-29	5	CVE-2021-26306 MISC
rsa -- archer	Archer before 6.9 P1 (6.9.0.1) contains an improper access control vulnerability in an API. A remote authenticated malicious administrative user can potentially exploit this vulnerability to gather information about the system, and may use this information in subsequent attacks.	2021-01-29	4	CVE-2020-29538 CONFIRM MISC
rsa -- archer	Archer before 6.8 P2 (6.8.0.2) is affected by an open redirect vulnerability. A remote privileged attacker may potentially redirect legitimate users to arbitrary web sites and conduct phishing attacks. The attacker could then steal the victims' credentials and silently authenticate them to the Archer application without the victims realizing an attack occurred.	2021-01-29	4.9	CVE-2020-29537 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rsa -- archer	Archer before 6.8 P2 (6.8.0.2) is affected by a path exposure vulnerability. A remote authenticated malicious attacker with access to service files may obtain sensitive information to use it in further attacks.	2021-01-29	4	CVE-2020-29536 CONFIRM MISC
solarwinds -- serv-u	SolarWinds Serv-U before 15.2.2 allows Authenticated Directory Traversal.	2021-02-03	6.5	CVE-2020-27994 CONFIRM MISC
squaredup -- squaredup	A username enumeration issue was discovered in SquaredUp before version 4.6.0. The login functionality was implemented in a way that would enable a malicious user to guess valid username due to a different response time from invalid usernames.	2021-02-03	4.3	CVE-2020-9389 CONFIRM
tk-star -- q90_junior_gps_horloge_firmware	An issue was discovered on TK-Star Q90 Junior GPS horloge 3.1042.9.8656 devices. Any SIM card used with the device cannot have a PIN configured. If a PIN is configured, the device simply produces a "Remove PIN and restart!" message, and	2021-02-01	4.6	CVE-2019-20473

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cannot be used. This makes it easier for an attacker to use the SIM card by stealing the device.			MISC MISC
tk-star -- q90_junior_gps_horloge_firmware	An issue was discovered on TK-Star Q90 Junior GPS horloge 3.1042.9.8656 devices. It performs actions based on certain SMS commands. This can be used to set up a voice communication channel from the watch to any telephone number, initiated by sending a specific SMS and using the default password, e.g., pw,<password>,call,<mobile_number> triggers an outbound call from the watch. The password is sometimes available because of CVE-2019-20471.	2021-02-01	5	CVE-2019-20470 MISC MISC
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain x64 agent hofitx information.	2021-02-04	5	CVE-2021-25240 N/A N/A N/A N/A
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One (on-prem), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about x86 agent hotfixes.	2021-02-04	5	CVE-2021-25239 N/A

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				N/A N/A N/A
trendmicro -- apex_one	An improper access control information disclosure vulnerability in Trend Micro Apex One, Apex One as a Service, OfficeScan XG SP1, and Worry-Free Business Security could allow an unauthenticated user to create a bogus agent on an affected server that could be used then make valid configuration queries.	2021-02-04	6.4	CVE-2021-25246 N/A N/A N/A N/A
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific configuration download file.	2021-02-04	5	CVE-2021-25233 N/A N/A N/A N/A
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One (on-prem) could allow an unauthenticated user to obtain information about the managing port used by agents.	2021-02-04	5	CVE-2021-25237

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				N/A N/A
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain information about the SQL database.	2021-02-04	5	CVE-2021-25232 N/A N/A N/A
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain information about a content inspection configuration file.	2021-02-04	5	CVE-2021-25235 N/A N/A N/A
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain patch level information.	2021-02-04	5	CVE-2021-25243 N/A N/A N/A N/A

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific notification configuration file.	2021-02-04	5	CVE-2021-25234 N/A N/A N/A N/A
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain version and build information.	2021-02-04	5	CVE-2021-25242 N/A N/A N/A N/A
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain information about the contents of a scan connection exception file.	2021-02-04	5	CVE-2021-25230 N/A N/A N/A

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific hotfix history file.	2021-02-04	5	CVE-2021-25231 N/A N/A N/A N/A
trendmicro -- apex_one	A server-side request forgery (SSRF) information disclosure vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to locate online agents via a sweep.	2021-02-04	5	CVE-2021-25241 N/A N/A N/A
trendmicro -- officescan	An improper access control information disclosure vulnerability in Trend Micro OfficeScan XG SP1 and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about an agent's managing port.	2021-02-04	5	CVE-2021-25238 N/A N/A N/A
trendmicro -- officescan	A server-side request forgery (SSRF) information disclosure vulnerability in Trend Micro OfficeScan XG SP1 and Worry-	2021-02-04	5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Free Business Security 10.0 SP1 could allow an unauthenticated user to locate online agents via a specific sweep.			25236 N/A N/A N/A
uip_project -- uip	An issue was discovered in uIP through 1.0, as used in Contiki and Contiki-NG. Domain name parsing lacks bounds checks, allowing an attacker to corrupt memory with crafted DNS packets.	2021-02-02	5	CVE-2020-24335 MISC MISC MISC MISC MISC
wikindx_project -- wikindx	A cross-site scripting (XSS) vulnerability in many forms of Wikindx before 5.7.0 and 6.x through 6.4.0 allows remote attackers to inject arbitrary web script or HTML via the message parameter to index.php?action=initLogon or modules/admin/DELETEIMAGES.php.	2021-02-01	4.3	CVE-2021-3340 MISC MISC
wwbn -- avideo	AVideo Platform is an open-source Audio and Video platform. It is similar to a self-hosted YouTube. In AVideo Platform before version 10.2 there is an authorization bypass vulnerability which enables an ordinary user to get admin control. This is fixed in	2021-02-01	6.5	CVE-2021-21286 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	version 10.2. All queries now remove the pass hash and the recoverPass hash.			CONFIRM
yccms -- yccms	Directory traversal vulnerability in the yccms 3.3 project. The delete, deletesite, and deleteAll functions' improper judgment of the request parameters, triggers a directory traversal vulnerability.	2021-02-01	6.4	CVE-2020-20290 MISC
zivautomation -- 4cct-ea6-334126bf_firmware	ZIV Automation 4CCT-EA6-334126BF firmware version 3.23.80.27.36371, allows an unauthenticated, remote attacker to cause a denial of service condition on the device. An attacker could exploit this vulnerability by sending specific packets to the port 7919.	2021-01-29	5	CVE-2021-25909 CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
altn -- mdaemon_webmail	Stored cross-site scripting (XSS) in file attachment field in	2021-02-03	3.5	CVE-2020-

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	MDaemon webmail 19.5.5 allows an attacker to execute code on the email recipient side while forwarding an email to perform potentially malicious activities.			18723 MISC MISC
altn -- mdaemon_webmail	Authenticated stored cross-site scripting (XSS) in the contact name field in the distribution list of MDaemon webmail 19.5.5 allows an attacker to executes code and perform a XSS attack while opening a contact list.	2021-02-03	3.5	CVE-2020-18724 MISC MISC
google -- android	In RT regmap driver, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05453809.	2021-02-03	2.1	CVE-2021-0352 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In ccu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05377188.	2021-02-04	2.1	CVE-2021-0347 MISC
hitachi -- vantara_pentaho	The dashboard Editor in Hitachi Vantara Pentaho through 7.x - 8.x contains a reflected Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'pho:title' attribute of 'dashboardXml' parameter. Remediated in >= 7.1.0.25, >= 8.2.0.6, and >= 8.3.0.0 GA.	2021-01-29	3.5	CVE-2020-24664 MISC MISC
hitachi -- vantara_pentaho	The Analysis Report in Hitachi Vantara Pentaho through 7.x - 8.x contains a stored Cross-site	2021-01-29	3.5	CVE-2020-24666

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'Display Name' parameter. Remediated in >= 9.1.0.1			MISC MISC
hitachi -- vantara_pentaho	The New Analysis Report in Hitachi Vantara Pentaho through 7.x - 8.x contains a DOM-based Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'Analysis Report Description' field in 'About this Report' section. Remediated in >= 8.3.0.9, >= 9.0.0.1, and >= 9.1.0.0 GA.	2021-01-29	3.5	CVE-2020-24669 MISC MISC
hitachi -- vantara_pentaho	The Dashboard Editor in Hitachi Vantara Pentaho through 7.x - 8.x contains a reflected Cross-site scripting vulnerability, which allows an authenticated	2021-01-29	3.5	CVE-2020-24670 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'type' attribute of 'dashboardXml' parameter. Remediated in >= 7.1.0.25, >= 8.2.0.6, and >= 8.3.0.0 GA.			
ibm -- api_connect	Certain IBM API Connect 10.0.0.0 through 10.0.1.0 and 2018.4.1.0 through 2018.4.1.13 configurations can result in sensitive information in the URL fragment identifiers. This information can be cached in the intermediate nodes like proxy servers, cdn, logging platforms, etc. An attacker can make use of this information to perform attacks by impersonating a user. IBM X-Force ID: 185510.	2021-02-04	3.8	CVE-2020-4640 XF CONFIRM
ibm -- api_connect	IBM API Connect 10.0.0.0 through 10.0.1.0 and 2018.4.1.0 through 2018.4.1.13 is vulnerable to cross-site scripting. This vulnerability	2021-02-04	3.5	CVE-2020-4825 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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: 189839.			
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.3 and 7.4 in some configurations may be vulnerable to a temporary denial of service attack when sent particular payloads. IBM X-Force ID: 194178.	2021-02-04	3.3	CVE-2020-5032 XF CONFIRM
linux -- linux_kernel	nbd_add_socket in drivers/block/nbd.c in the Linux kernel through 5.10.12 has an ndb_queue_rq use-after-free that could be triggered by local attackers (with access to the nbd device) via an I/O request at a certain point during device setup, aka CID-b98e762e3d71.	2021-02-01	2.1	CVE-2021-3348 MLIST MISC MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
nextcloud -- nextcloud_server	A missing link validation in Nextcloud Server before 20.0.2, 19.0.5, 18.0.11 allows execution of a stored XSS attack using Internet Explorer when saving a 'javascript:' URL in markdown format.	2021-02-03	3.5	CVE-2020-8294 CONFIRM CONFIRM
phpgurukul -- daily_expense_tracker_system	PHPGurukul Daily Expense Tracker System 1.0 is vulnerable to stored XSS via the add-expense.php Item parameter.	2021-01-29	3.5	CVE-2021-26304 MISC
pryaniki -- pryaniki	A cross-site scripting (XSS) vulnerability in Pryaniki 6.44.3 allows remote authenticated users to upload an arbitrary file. The JavaScript code will execute when someone visits the attachment.	2021-02-02	3.5	CVE-2021-3395 MISC MISC
raw-cpuid_project -- raw-cpuid	An issue was discovered in the raw-cpuid crate before 9.0.0 for Rust. It allows __cpuid_count() calls even if the processor does not support the CPUID	2021-01-29	2.1	CVE-2021-26307 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	instruction, which is unsound and causes a deterministic crash.			
rsa -- archer	Archer before 6.8 P4 (6.8.0.4) contains a stored XSS vulnerability. A remote authenticated malicious Archer user could potentially exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When application users access the corrupted data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application.	2021-01-29	3.5	CVE-2020-29535 CONFIRM MISC
solarwinds -- serv-u	SolarWinds Serv-U before 15.2.2 allows authenticated reflected XSS.	2021-02-03	3.5	CVE-2020-35482 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
solarwinds -- serv-u	SolarWinds Serv-U before 15.2.2 allows Authenticated Stored XSS.	2021-02-03	3.5	CVE-2020-28001 CONFIRM MISC
squaredup -- squaredup	SquaredUp allowed Stored XSS before version 4.6.0. A user was able to create a dashboard that executed malicious content in iframe or by uploading an SVG that contained a script.	2021-02-03	3.5	CVE-2020-9390 CONFIRM
trendmicro -- apex_one	An out-of-bounds read information disclosure vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security (10.0 SP1 and Services) could allow an attacker to disclose sensitive information about a named pipe. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2021-02-04	2.1	CVE-2021-25248 N/A N/A N/A N/A

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zivautomation -- 4cct-ea6-334126bf_firmware	Improper Authentication vulnerability in the cookie parameter of ZIV AUTOMATION 4CCT-EA6-334126BF allows a local attacker to perform modifications in several parameters of the affected device as an authenticated user.	2021-01-29	3.3	CVE-2021-25910 CONFIRM