BULLETIN (SB21-095)
VULNERABILITY SUMMARY FOR THE WEEK OF
29TH MARCH, 2021

Bulletin (SB21-095)
Vulnerability Summary for the Week of March 29, 2021

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.
The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by 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 Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis . The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available

HIGH Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arubanetworks -- instant	A remote buffer overflow vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.17 and below; Aruba Instant 6.5.x: 6.5.4.16 and below; Aruba Instant 8.3.x: 8.3.0.12 and below; Aruba Instant 8.5.x: 8.5.0.6 and below; Aruba Instant 8.6.x: 8.6.0.2 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	10	CVE-2019-5319 MISC
arubanetworks -- instant	A remote buffer overflow vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.17 and below; Aruba Instant 6.5.x: 6.5.4.16 and below; Aruba Instant 8.3.x: 8.3.0.12 and below; Aruba Instant 8.5.x: 8.5.0.6 and below; Aruba Instant 8.6.x: 8.6.0.2 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-29	9	CVE-2021-25144 MISC
arubanetworks -- instant	A remote buffer overflow vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.17 and below; Aruba Instant 6.5.x: 6.5.4.16 and below; Aruba Instant 8.3.x: 8.3.0.12 and below; Aruba Instant 8.5.x: 8.5.0.6 and below; Aruba Instant 8.6.x: 8.6.0.2 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	7.5	CVE-2021-25149 MISC
arubanetworks -- instant	A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.5.x: 6.5.4.17 and below; Aruba Instant 8.3.x: 8.3.0.13 and below; Aruba Instant 8.5.x: 8.5.0.10 and below; Aruba Instant 8.6.x: 8.6.0.5 and below; Aruba Instant 8.7.x: 8.7.0.0 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-29	10	CVE-2020-24636 MISC
arubanetworks -- instant	A remote arbitrary file modification vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.17 and below; Aruba Instant 6.5.x: 6.5.4.18 and below; Aruba Instant 8.3.x: 8.3.0.14 and below; Aruba Instant 8.5.x: 8.5.0.11 and below; Aruba Instant 8.6.x: 8.6.0.7 and below; Aruba Instant 8.7.x: 8.7.1.1 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	8.5	CVE-2021-25159 MISC
arubanetworks -- instant	A remote arbitrary file modification vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.17 and below; Aruba Instant 6.5.x: 6.5.4.18 and below; Aruba Instant 8.3.x: 8.3.0.14 and below; Aruba Instant 8.5.x: 8.5.0.11 and below; Aruba Instant 8.6.x: 8.6.0.6 and below; Aruba Instant 8.7.x: 8.7.1.0 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	8.5	CVE-2021-25155 MISC
arubanetworks -- instant	A remote arbitrary file modification vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.5.x: 6.5.4.17 and below; Aruba Instant 8.3.x: 8.3.0.13 and below; Aruba Instant 8.5.x: 8.5.0.10 and below; Aruba Instant 8.6.x: 8.6.0.4 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	8.5	CVE-2021-25148 MISC
arubanetworks -- instant	A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.5.x: 6.5.4.17 and below; Aruba Instant 8.3.x: 8.3.0.13 and below; Aruba Instant 8.5.x: 8.5.0.10 and below; Aruba Instant 8.6.x: 8.6.0.4 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	9	CVE-2021-25150 MISC
arubanetworks -- instant	A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.5.x: 6.5.4.17 and below; Aruba Instant 8.3.x: 8.3.0.13 and below; Aruba Instant 8.5.x: 8.5.0.10 and below; Aruba Instant 8.6.x: 8.6.0.5 and below; Aruba Instant 8.7.x: 8.7.0.0 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	9	CVE-2021-25146 MISC

arubanetworks -- instant	A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.17 and below; Aruba Instant 6.5.x: 6.5.4.18 and below; Aruba Instant 8.3.x: 8.3.0.14 and below; Aruba Instant 8.5.x: 8.5.0.11 and below; Aruba Instant 8.6.x: 8.6.0.7 and below; Aruba Instant 8.7.x: 8.7.1.1 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	9.3	CVE-2021-25162 MISC
arubanetworks -- instant	A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.5.x: 6.5.4.17 and below; Aruba Instant 8.3.x: 8.3.0.13 and below; Aruba Instant 8.5.x: 8.5.0.10 and below; Aruba Instant 8.6.x: 8.6.0.5 and below; Aruba Instant 8.7.x: 8.7.0.0 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-29	9	CVE-2020-24635 MISC
askey -- rtf3505vw-n1_br_sv_g000_r3505vwn1001_s32_7_firmware	Askey Fiber Router RTF3505VW-N1 BR_SV_g000_R3505VWN1001_s32_7 devices allow Remote Code Execution and retrieval of admin credentials to log into the Dashboard or login via SSH, leading to code execution as root.	2021-03-26	8.3	CVE-2020-28695 MISC
basercms -- basercms	baserCMS versions prior to 4.4.5 allows a remote attacker with an administrative privilege to execute arbitrary OS commands via unspecified vectors.	2021-03-26	9	CVE-2021-20682 MISC MISC
buddypress -- buddypress	BuddyPress is an open source WordPress plugin to build a community site. In releases of BuddyPress from 5.0.0 before 7.2.1 it's possible for a non-privileged, regular user to obtain administrator rights by exploiting an issue in the REST API members endpoint. The vulnerability has been fixed in BuddyPress 7.2.1. Existing installations of the plugin should be updated to this version to mitigate the issue.	2021-03-26	9	CVE-2021-21389 MISC MISC CONFIRM
ca -- ehealth_performance_manager	** UNSUPPORTED WHEN ASSIGNED ** CA eHealth Performance Manager through 6.3.2.12 is affected by Privilege Escalation via a Dynamically Linked Shared Object Library. To exploit the vulnerability, the ehealth user must create a malicious library in the writable RPATH, to be dynamically linked when the FtpCollector executable is run. The code in the library will be executed as the root user. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-03-26	7.2	CVE-2021-28249 MISC
freebsd -- freebsd	In FreeBSD 12.2-STABLE before r365767, 11.4-STABLE before r365769, 12.1-RELEASE before p10, 11.4-RELEASE before p4 and 11.3-RELEASE before p14 a number of AMD virtualization instructions operate on host physical addresses, are not subject to nested page table translation, and guest use of these instructions was not trapped.	2021-03-26	7.2	CVE-2020-7467 MISC
freebsd -- freebsd	In FreeBSD 12.2-STABLE before r368250, 11.4-STABLE before r368253, 12.2-RELEASE before p1, 12.1-RELEASE before p11 and 11.4-RELEASE before p5 rtsold(8) does not verify that the RDNSS option does not extend past the end of the received packet before processing its contents. While the kernel currently ignores such malformed packets, it passes them to userspace programs. Any programs expecting the kernel to do validation may be vulnerable to an overflow.	2021-03-29	10	CVE-2020-25577 MISC
freebsd -- freebsd	In FreeBSD 12.2-STABLE before r368250, 11.4-STABLE before r368253, 12.2-RELEASE before p1, 12.1-RELEASE before p11 and 11.4-RELEASE before p5 when processing a DNSSL option, rtsold(8) decodes domain name labels per an encoding specified in RFC 1035 in which the first octet of each label contains the label's length. rtsold(8) did not validate label lengths correctly and could overflow the destination buffer.	2021-03-29	10	CVE-2020-25583 MISC
freebsd -- freebsd	In FreeBSD 12.2-STABLE before r369312, 11.4-STABLE before r369313, 12.2-RELEASE before p4 and 11.4-RELEASE before p8 due to a race condition in the jail_remove(2) implementation, it may fail to kill some of the processes.	2021-03-26	8.5	CVE-2020-25581 MISC
freebsd -- freebsd	In FreeBSD 12.2-STABLE before r365772, 11.4-STABLE before r365773, 12.1-RELEASE before p10, 11.4-RELEASE before p4 and 11.3-RELEASE before p14 a ftpd(8) bug in the implementation of the file system sandbox, combined with capabilities available to an authenticated FTP user, can be used to escape the file system restriction configured in ftpchroot(5). Moreover, the bug allows a malicious client to gain root privileges.	2021-03-26	9	CVE-2020-7468 MISC

freebsd -- freebsd	In FreeBSD 12.2-STABLE before r369334, 11.4-STABLE before r369335, 12.2-RELEASE before p4 and 11.4-RELEASE before p8 when a process, such as jexec(8) or killall(1), calls jail_attach(2) to enter a jail, the jailed root can attach to it using ptrace(2) before the current working directory is changed.	2021-03-26	8.5	CVE-2020-25582 MISC
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r365010, 11.4-STABLE before r365011, 12.1-RELEASE before p9, 11.4-RELEASE before p3, and 11.3-RELEASE before p13, dhclient(8) fails to handle certain malformed input related to handling of DHCP option 119 resulting a heap overflow. The heap overflow could in principle be exploited to achieve remote code execution. The affected process runs with reduced privileges in a Capsicum sandbox, limiting the immediate impact of an exploit.	2021-03-26	7.5	CVE-2020-7461 MISC
gitjacker_project -- gitjacker	gitjacker before 0.1.0 allows remote attackers to execute arbitrary code via a crafted .git directory because of directory traversal.	2021-03-29	7.5	CVE-2021-29417 MISC MISC MISC
google -- android	A vulnerability in DSP driver prior to SMR Mar-2021 Release 1 allows attackers load arbitrary ELF libraries inside DSP.	2021-03-26	7.2	CVE-2021-25371 MISC CONFIRM
google -- android	An improper boundary check in DSP driver prior to SMR Mar-2021 Release 1 allows out of bounds memory access.	2021-03-26	7.2	CVE-2021-25372 MISC CONFIRM
grandstream -- grp2612_firmware	Grandstream GRP261x VoIP phone running firmware version 1.0.3.6 (Base) allow Authentication Bypass in its administrative web interface.	2021-03-29	10	CVE-2020-25218 MISC
grandstream -- grp2612_firmware	Grandstream GRP261x VoIP phone running firmware version 1.0.3.6 (Base) allows Command Injection as root in its administrative web interface.	2021-03-29	9	CVE-2020-25217 MISC
gridx_project -- gridx	Remote Code Execution Vulnerability in tests/support/stores/test_grid_filter.php in oria gridx 1.3, allows remote attackers to execute arbitrary code, via crafted value to the $query parameter.	2021-03-26	7.5	CVE-2020-19625 MISC MISC
kongchuanhujiao_project -- kongchuanhujiao	In github.com/kongchuanhujiao/server before version 1.3.21 there is an authentication Bypass by Primary Weakness vulnerability. All users are impacted. This is fixed in version 1.3.21.	2021-03-26	7.5	CVE-2021-21403 MISC CONFIRM
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.11.9. drivers/vhost/vdpa.c has a use-after-free because v->config_ctx has an invalid value upon re-opening a character device, aka CID-f6bbf0010ba0.	2021-03-26	7.2	CVE-2021-29266 MISC MISC
mitel -- micontact_center_enterprise	The Enterprise License Manager portal in Mitel MiContact Center Enterprise before 9.4 could allow a user to access restricted files and folders due to insufficient access control. A successful exploit could allow an attacker to view and modify application data via Directory Traversal.	2021-03-29	7.5	CVE-2021-26714 CONFIRM
mongo-express_project -- mongo-express	mongo-express before 1.0.0 offers support for certain advanced syntax but implements this in an unsafe way. NOTE: this may overlap CVE-2019-10769.	2021-03-30	7.5	CVE-2020-24391 MISC MISC
netgear -- d6220_firmware	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6400 and R6700 firmware version 1.0.4.98 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the upnpd service, which listens on UDP port 1900 by default. A crafted MX header field in an SSDP message can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-11851.	2021-03-29	8.3	CVE-2021-27239 N/A N/A

netgear -- prosafe_network_management_system	This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System 1.6.0.26. Authentication is not required to exploit this vulnerability. The specific flaw exists within the MFileUploadController class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-12124.	2021-03-29	10	CVE-2021-27274 MISC MISC
netgear -- prosafe_network_management_system	This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System 1.6.0.26. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the SettingConfigController class. When parsing the fileName parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-12121.	2021-03-29	9	CVE-2021-27273 MISC MISC
netgear -- prosafe_network_management_system	This vulnerability allows remote attackers to delete arbitrary files on affected installations of NETGEAR ProSAFE Network Management System 1.6.0.26. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the ReportTemplateController class. When parsing the path parameter, the process does not properly validate a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-12123.	2021-03-29	7.5	CVE-2021-27272 MISC MISC
salesforce -- mule	MuleSoft is aware of a Remote Code Execution vulnerability affecting certain versions of a Mule runtime component that may affect both CloudHub and on-premise customers. Versions affected: Mule 4.1.x and 4.2.x runtime released before February 2, 2021.	2021-03-26	7.5	CVE-2021-1626 MISC
salesforce -- mule	MuleSoft is aware of a Server Side Request Forgery vulnerability affecting certain versions of a Mule runtime component that may affect both CloudHub and on-premise customers. This affects: Mule 3.8.x,3.9.x,4.x runtime released before February 2, 2021.	2021-03-26	7.5	CVE-2021-1627 MISC
salesforce -- mule	MuleSoft is aware of a XML External Entity (XXE) vulnerability affecting certain versions of a Mule runtime component that may affect both CloudHub and on-premise customers. Affected versions: Mule 4.x runtime released before February 2, 2021.	2021-03-26	7.5	CVE-2021-1628 MISC
simple_college_project -- simple_college	A SQL injection vulnerability in Simple College Website 1.0 allows remote unauthenticated attackers to bypass the admin authentication mechanism in college_website/admin/ajax.php?action=login, thus gaining access to the website administrative panel.	2021-03-31	7.5	CVE-2020-28172 MISC MISC MISC MISC
solarwinds -- patch_manager	This vulnerability allows local attackers to escalate privileges on affected installations of SolarWinds Patch Manager 2020.2.1. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the DataGridService WCF service. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of Administrator. Was ZDI-CAN-12009.	2021-03-29	7.2	CVE-2021-27240 N/A
tp-link -- archer_a7_firmware	This vulnerability allows a firewall bypass on affected installations of TP-Link Archer A7 prior to Archer C7(US)_V5_210125 and Archer A7(US)_V5_200220 AC1750 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of IPv6 connections. The issue results from the lack of proper filtering of IPv6 SSH connections. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-12309.	2021-03-29	9.3	CVE-2021-27245 N/A
underscorejs -- underscore	The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Execution via the template function, particularly when a variable property is passed as an argument as it is not sanitized.	2021-03-29	7.5	CVE-2021-23358 MISC MLIST MISC MISC MISC MISC DEBIAN

upx_project -- upx	A flaw was found in upx canPack in p_lx_elf.cpp in UPX 3.96. This flaw allows attackers to cause a denial of service (SEGV or buffer overflow and application crash) or possibly have unspecified other impacts via a crafted ELF. The highest threat from this vulnerability is to system availability.	2021-03-26	8.3	CVE-2021-20285 MISC MISC
xerox -- altalink_b8045_firmware	Xerox AltaLink B80xx before 103.008.020.23120, C8030/C8035 before 103.001.020.23120, C8045/C8055 before 103.002.020.23120 and C8070 before 103.003.020.23120 has several SQL injection vulnerabilities.	2021-03-29	7.5	CVE-2021-28668 CONFIRM
zte -- zxhn_f623_firmware	A ZTE product has a DoS vulnerability. A remote attacker can amplify traffic by sending carefully constructed IPv6 packets to the affected devices, which eventually leads to device denial of service. This affects:<ZXHN F623><All versions up to V6.0.0P3T33>	2021-03-29	7.8	CVE-2021-21727 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
\@thi.ng\/egf_project -- \@thi.ng\/egf	Potential for arbitrary code execution in npm package @thi.ng/egf `#gpg`-tagged property values (only if `decrypt: true` option is enabled). PR with patch has been submitted and will has been released as of v0.4.0 By default the EGF parse functions do NOT attempt to decrypt values (since GPG only available in non-browser env). However, if GPG encrypted values are used/required: 1. Perform a regex search for `#gpg`-tagged values in the EGF source file/string and check for backtick (\`) chars in the encrypted value string 2. Replace/remove them or skip parsing if present.	2021-03-30	6.5	CVE-2021-21412 MISC MISC CONFIRM MISC
accusoft -- imagegear	An out-of-bounds write vulnerability exists in the SGI format buffer size processing functionality of Accusoft ImageGear 19.8. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	2021-03-31	6.8	CVE-2021-21782 MISC
acexy -- wireless-n_wifi_repeater_firmware	The Acexy Wireless-N WiFi Repeater REV 1.0 (28.08.06.1) Web management administrator password can be changed by sending a specially crafted HTTP GET request. The administrator username has to be known (default:admin) whereas no previous authentication is required.	2021-03-29	5	CVE-2021-28936 MISC MISC MISC
acexy -- wireless-n_wifi_repeater_firmware	The /password.html page of the Web management interface of the Acexy Wireless-N WiFi Repeater REV 1.0 (28.08.06.1) contains the administrator account password in plaintext. The page can be intercepted on HTTP.	2021-03-29	5	CVE-2021-28937 MISC MISC
algolplus -- advanced_order_export	Advanced Order Export before 3.1.8 for WooCommerce allows XSS, a different vulnerability than CVE-2020-11727.	2021-03-31	4.3	CVE-2021-27349 MISC
apache -- druid	Apache Druid allows users to read data from other database systems using JDBC. This functionality is to allow trusted users with the proper permissions to set up lookups or submit ingestion tasks. The MySQL JDBC driver supports certain properties, which, if left unmitigated, can allow an attacker to execute arbitrary code from a hacker-controlled malicious MySQL server within Druid server processes. This issue was addressed in Apache Druid 0.20.2	2021-03-30	6.5	CVE-2021-26919 MLIST MISC MLIST MLIST
apache -- tika	A carefully crafted or corrupt file may trigger an infinite loop in Tika's MP3Parser up to and including Tika 1.25. Apache Tika users should upgrade to 1.26 or later.	2021-03-31	4.3	CVE-2021-28657 MISC
arubanetworks -- instant	A remote cross-site scripting (xss) vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.17 and below; Aruba Instant 6.5.x: 6.5.4.18 and below; Aruba Instant 8.3.x: 8.3.0.14 and below; Aruba Instant 8.5.x: 8.5.0.11 and below; Aruba Instant 8.6.x: 8.6.0.7 and below; Aruba Instant 8.7.x: 8.7.1.1 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	4.3	CVE-2021-25161 MISC
arubanetworks -- instant	A remote arbitrary file modification vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.17 and below; Aruba Instant 6.5.x: 6.5.4.18 and below; Aruba Instant 8.3.x: 8.3.0.14 and below; Aruba Instant 8.5.x: 8.5.0.11 and below; Aruba Instant 8.6.x: 8.6.0.7 and below; Aruba Instant 8.7.x: 8.7.1.1 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	4	CVE-2021-25160 MISC
arubanetworks -- instant	A remote arbitrary file read vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.17 and below; Aruba Instant 6.5.x: 6.5.4.18 and below; Aruba Instant 8.3.x: 8.3.0.14 and below; Aruba Instant 8.5.x: 8.5.0.11 and below; Aruba Instant 8.6.x: 8.6.0.6 and below; Aruba Instant 8.7.x: 8.7.1.0 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	4	CVE-2021-25157 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arubanetworks -- instant	A remote arbitrary directory create vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.17 and below; Aruba Instant 6.5.x: 6.5.4.18 and below; Aruba Instant 8.3.x: 8.3.0.14 and below; Aruba Instant 8.5.x: 8.5.0.11 and below; Aruba Instant 8.6.x: 8.6.0.6 and below; Aruba Instant 8.7.x: 8.7.1.0 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	4	CVE-2021-25156 MISC
arubanetworks -- instant	A local authentication bypass vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.18 and below; Aruba Instant 6.5.x: 6.5.4.15 and below; Aruba Instant 8.3.x: 8.3.0.11 and below; Aruba Instant 8.4.x: 8.4.0.5 and below; Aruba Instant 8.5.x: 8.5.0.6 and below; Aruba Instant 8.6.x: 8.6.0.2 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-29	4.6	CVE-2019-5317 MISC
arubanetworks -- instant	A remote denial of service (dos) vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 8.3.x: 8.3.0.12 and below; Aruba Instant 8.5.x: 8.5.0.9 and below; Aruba Instant 8.6.x: 8.6.0.4 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-29	5	CVE-2021-25143 MISC
arubanetworks -- instant	A remote arbitrary file read vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.5.x: 6.5.4.18 and below; Aruba Instant 8.3.x: 8.3.0.14 and below; Aruba Instant 8.5.x: 8.5.0.11 and below; Aruba Instant 8.6.x: 8.6.0.7 and below; Aruba Instant 8.7.x: 8.7.1.1 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	4.3	CVE-2021-25158 MISC
braces_project -- braces	A vulnerability was found in Braces versions prior to 2.3.1. Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) attacks.	2021-03-30	5	CVE-2018-1109 MISC MISC
btcpayserver -- btcpay_server	BTCPay Server before 1.0.6.0, when the payment button is used, has a privacy vulnerability.	2021-03-26	5	CVE-2021-29249 MISC MISC
ca -- ehealth	** UNSUPPORTED WHEN ASSIGNED ** CA eHealth Performance Manager through 6.3.2.12 is affected by Improper Restriction of Excessive Authentication Attempts. An attacker is able to perform an arbitrary number of /web/frames/ authentication attempts using different passwords, and eventually gain access to a targeted account, NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-03-26	5	CVE-2021-28248 MISC
ca -- ehealth	** UNSUPPORTED WHEN ASSIGNED ** CA eHealth Performance Manager through 6.3.2.12 is affected by Privilege Escalation via a Dynamically Linked Shared Object Library. A regular user must create a malicious library in the writable RPATH, to be dynamically linked when the emtgtctl2 executable is run. The code in the library will be executed as the ehealth user. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-03-26	4.4	CVE-2021-28246 MISC
ca -- ehealth_performance_manager	** UNSUPPORTED WHEN ASSIGNED ** CA eHealth Performance Manager through 6.3.2.12 is affected by Privilege Escalation via a setuid (and/or setgid) file. When a component is run as an argument of the runpicEhealth executable, the script code will be executed as the ehealth user. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-03-26	4.6	CVE-2021-28250 MISC
cncf -- container_network_interface	An improper limitation of path name flaw was found in containernetworking/cni in versions before 0.8.1. When specifying the plugin to load in the 'type' field in the network configuration, it is possible to use special elements such as "../" separators to reference binaries elsewhere on the system. This flaw allows an attacker to execute other existing binaries other than the cni plugins/types, such as 'reboot'. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	2021-03-26	6.5	CVE-2021-20206 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
douzone -- nbbdownloader.ocx	NBBDownloader.ocx ActiveX Control in Groupware contains a vulnerability that could allow remote files to be downloaded and executed by setting the arguments to the activex method. A remote attacker could induce a user to access a crafted web page, causing damage such as malicious code infection.	2021-03-29	6.8	CVE-2020-7850 MISC MISC
endian_trait_project -- endian_trait	An issue was discovered in the endian_trait crate through 2021-01-04 for Rust. A double drop can occur when a user-provided Endian impl panics.	2021-04-01	5	CVE-2021-29929 MISC
eterna -- ircii	ircII before 20210314 allows remote attackers to cause a denial of service (segmentation fault and client crash, disconnecting the victim from an IRC server) via a crafted CTCP UTC message.	2021-03-30	5	CVE-2021-29376 MISC MLIST MISC
ffmpeg -- ffmpeg	Buffer overflow vulnerability in sniff_channel_order function in aacdec_template.c in ffmpeg 3.1.2, allows attackers to execute arbitrary code (local).	2021-03-30	4.6	CVE-2020-24995 MISC MISC MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 10.1.0.37527. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-12270.	2021-03-30	4.3	CVE-2021-27262 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.1.0.37527. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12295.	2021-03-30	6.8	CVE-2021-27268 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 10.1.0.37527. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-12292.	2021-03-30	4.3	CVE-2021-27265 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 10.1.0.37527. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-12291.	2021-03-30	4.3	CVE-2021-27264 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.1.0.37527. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue	2021-03-30	6.8	CVE-2021-27271 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12438.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.1.0.37527. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPEG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12230.	2021-03-30	6.8	CVE-2021-27270 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.1.0.37527. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process Was ZDI-CAN-12390.	2021-03-30	6.8	CVE-2021-27269 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 10.1.0.37527. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-12293.	2021-03-30	4.3	CVE-2021-27266 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.1.0.37527. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12269.	2021-03-30	6.8	CVE-2021-27261 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 10.1.0.37527. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-12290.	2021-03-30	4.3	CVE-2021-27263 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.1.0.37527. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12294.	2021-03-30	6.8	CVE-2021-27267 MISC MISC
freebsd -- freebsd	In FreeBSD 12.2-STABLE before r368969, 11.4-STABLE before r369047, 12.2-RELEASE before p3, 12.1-RELEASE before p13 and 11.4-RELEASE before p7 several file systems were not properly initializing the d_off field of the dirent structures returned by VOP_READDIR. In particular, tmpfs(5), smbfs(5), autofs(5) and mqueuefs(5) were failing to do so. As a result, eight uninitialized kernel stack bytes may be leaked to userspace by these file systems.	2021-03-26	5	CVE-2020-25578 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r364644, 11.4-STABLE before r364651, 12.1-RELEASE before p9, 11.4-RELEASE before p3, and 11.3-RELEASE before p13, improper handling in the kernel causes a use-after-free bug by sending large user messages from multiple threads on the same SCTP socket. The use-after-free situation may result in unintended kernel behaviour including a kernel panic.	2021-03-26	4.9	CVE-2020-7463 MISC
freebsd -- freebsd	In 11.4-PRERELEASE before r360733 and 11.3-RELEASE before p13, improper mbuf handling in the kernel causes a use-after-free bug by sending IPv6 Hop-by-Hop options over the loopback interface. The use-after-free situation may result in unintended kernel behaviour including a kernel panic.	2021-03-26	4.9	CVE-2020-7462 MISC
freebsd -- freebsd	In FreeBSD 12.2-STABLE before r369346, 11.4-STABLE before r369345, 12.2-RELEASE before p4 and 11.4-RELEASE before p8 a regression in the login.access(5) rule processor has the effect of causing rules to fail to match even when they should not. This means that rules denying access may be ignored.	2021-03-26	5	CVE-2020-25580 MISC
freebsd -- freebsd	In FreeBSD 12.2-STABLE before r368969, 11.4-STABLE before r369047, 12.2-RELEASE before p3, 12.1-RELEASE before p13 and 11.4-RELEASE before p7 msdosfs(5) was failing to zero-fill a pair of padding fields in the dirent structure, resulting in a leak of three uninitialized bytes.	2021-03-26	5	CVE-2020-25579 MISC
freebsd -- freebsd	In FreeBSD 12.2-STABLE before r365730, 11.4-STABLE before r365738, 12.1-RELEASE before p10, 11.4-RELEASE before p4, and 11.3-RELEASE before p14, a programming error in the ure(4) device driver caused some Realtek USB Ethernet interfaces to incorrectly report packets with more than 2048 bytes in a single USB transfer as having a length of only 2048 bytes. An adversary can exploit this to cause the driver to misinterpret part of the payload of a large packet as a separate packet, and thereby inject packets across security boundaries such as VLANs.	2021-03-26	5	CVE-2020-7464 MISC
gistpad_project -- gistpad	GistPad before 0.2.7 allows a crafted workspace folder to change the URL for the Gist API, which leads to leakage of GitHub access tokens.	2021-03-30	5	CVE-2021-29642 MISC MISC
gitlab -- gitlab	Improper authorization in GitLab 12.8+ allows a guest user in a private project to view tag data that should be inaccessible on the releases page	2021-03-26	4	CVE-2021-22172 CONFIRM MISC MISC
gitlab -- gitlab	An issue has been discovered in GitLab affecting all versions starting from 13.4. Improper access control allows unauthorized users to access details on analytic pages.	2021-03-26	4	CVE-2021-22180 CONFIRM MISC MISC
gnu -- binutils	A flaw was found in GNU Binutils 2.35.1, where there is a heap-based buffer overflow in _bfd_elf_slurp_secondary_reloc_section in elf.c due to the number of symbols not calculated correctly. The highest threat from this vulnerability is to system availability.	2021-03-26	4.3	CVE-2021-20284 MISC MISC
gnu -- tar	A flaw was found in the src/list.c of tar 1.33 and earlier. This flaw allows an attacker who can submit a crafted input file to tar to cause uncontrolled consumption of memory. The highest threat from this vulnerability is to system availability.	2021-03-26	4.3	CVE-2021-20193 MISC MISC MISC
google -- android	An incorrect implementation handling file descriptor in dpu driver prior to SMR Mar-2021 Release 1 results in memory corruption leading to kernel panic.	2021-03-26	4.9	CVE-2021-25370 MISC CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cloud_pak_for_automation	IBM Cloud Pak for Automation 20.0.2 and 20.0.3 IF002 are vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 197504.	2021-03-30	5.5	CVE-2021-20482 XF CONFIRM
ibm -- engineering_insights	IBM Jazz Foundation Products are vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 198059.	2021-03-30	5.5	CVE-2021-20502 XF CONFIRM
ibm -- urbancode_deploy	IBM UrbanCode Deploy (UCD) 6.2.7.9, 7.0.5.4, and 7.1.1.1 could allow an authenticated user to initiate a plugin or compare process resources that they should not have access to. IBM X-Force ID: 190293.	2021-03-30	5.5	CVE-2020-4848 XF CONFIRM
ilch -- ilch_cms	An open redirect vulnerability in Ilch CMS version 2.1.42 allows attackers to redirect users to an attacker's site after a successful login.	2021-03-29	4.9	CVE-2021-27352 MISC MISC MISC
imagemagick -- imagemagick	A heap based buffer overflow in coders/tiff.c may result in program crash and denial of service in ImageMagick before 7.0.10-45.	2021-03-26	4.3	CVE-2020-27829 MISC MISC
insma -- wifi_mini_spy_1080p_hd_security_ip_camera_firmware	An issue was discovered in INSMA Wifi Mini Spy 1080P HD Security IP Camera 1.9.7 B. A local attacker can execute arbitrary code via editing the 'recdata.db' file to call a specially crafted GoAhead ASP-file on the SD card.	2021-03-30	4.6	CVE-2020-19642 MISC
insma -- wifi_mini_spy_1080p_hd_security_ip_camera_firmware	Cross Site Scripting (XSS) vulnerability in INSMA Wifi Mini Spy 1080P HD Security IP Camera 1.9.7 B via all fields in the FTP settings page to the "goform/formSetFtpCfg" settings page.	2021-03-30	4.3	CVE-2020-19643 MISC
insma -- wifi_mini_spy_1080p_hd_security_ip_camera_firmware	Cross Site Request Forgery (CSRF) vulnerability in INSMA Wifi Mini Spy 1080P HD Security IP Camera 1.9.7 B, via all fields to WebUI.	2021-03-30	6.8	CVE-2020-19639 MISC
insma -- wifi_mini_spy_1080p_hd_security_ip_camera_firmware	An issue was discovered in INSMA Wifi Mini Spy 1080P HD Security IP Camera 1.9.7 B. An unauthenticated attacker can reboot the device causing a Denial of Service, via a hidden reboot command to '/media/?action=cmd'.	2021-03-30	5	CVE-2020-19640 MISC
insma -- wifi_mini_spy_1080p_hd_security_ip_camera_firmware	An issue was discovered in INSMA Wifi Mini Spy 1080P HD Security IP Camera 1.9.7 B. Authenticated attackers with the "Operator" Privilege can gain admin privileges via a crafted request to '/goform/formUserMng'.	2021-03-30	6.5	CVE-2020-19641 MISC
is-my-json-valid_project -- is-my-json-valid	It was discovered that the is-my-json-valid JavaScript library used an inefficient regular expression to validate JSON fields defined to have email format. A specially crafted JSON file could cause it to consume an excessive amount of CPU time when validated.	2021-03-30	5	CVE-2018-1107 MISC MISC
jenkins -- build_with_parameters	A cross-site request forgery (CSRF) vulnerability in Jenkins Build With Parameters Plugin 1.5 and earlier allows attackers to build a project with attacker-specified parameters.	2021-03-30	6.8	CVE-2021-21629 MLIST CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- cloud_statistics	Jenkins Cloud Statistics Plugin 0.26 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission and knowledge of random activity IDs to view related provisioning exception error messages.	2021-03-30	4	CVE-2021-21631 MLIST CONFIRM
jenkins -- jabber_\(xmpp\)_notifier_and_control	Jenkins Jabber (XMPP) notifier and control Plugin 1.41 and earlier stores passwords unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	2021-03-30	4	CVE-2021-21634 MLIST CONFIRM
jenkins -- owasp_dependency-track	A cross-site request forgery (CSRF) vulnerability in Jenkins OWASP Dependency-Track Plugin 3.1.0 and earlier allows attackers to connect to an attacker-specified URL, capturing credentials stored in Jenkins.	2021-03-30	6.8	CVE-2021-21633 MLIST CONFIRM
jenkins -- owasp_dependency-track	A missing permission check in Jenkins OWASP Dependency-Track Plugin 3.1.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL, capturing credentials stored in Jenkins.	2021-03-30	4	CVE-2021-21632 MLIST CONFIRM
jenkins -- team_foundation_server	A cross-site request forgery (CSRF) vulnerability in Jenkins Team Foundation Server Plugin 5.157.1 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2021-03-30	6.8	CVE-2021-21638 MLIST CONFIRM
kill-by-port_project -- kill-by-port	This affects the package kill-by-port before 0.0.2. If (attacker-controlled) user input is given to the killByPort function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-03-30	6.5	CVE-2021-23363 CONFIRM CONFIRM CONFIRM
librit -- passhport	app/views_mod/user/user.py in LibrIT PaSSHport through 2.5 is affected by LDAP Injection. There is an information leak through the crafting of special queries, escaping the provided search filter because user input gets no sanitization.	2021-03-26	4	CVE-2021-3027 MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel through 5.11.10. drivers/net/ethernet/freescale/gianfar.c in the Freescale Gianfar Ethernet driver allows attackers to cause a system crash because a negative fragment size is calculated in situations involving an rx queue overrun when jumbo packets are used and NAPI is enabled, aka CID-d8861bab48b6.	2021-03-26	4.7	CVE-2021-29264 MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.11.7. usbip_sockfd_store in drivers/usb/usbip/stub_dev.c allows attackers to cause a denial of service (GPF) because the stub-up sequence has race conditions during an update of the local and shared status, aka CID-9380afd6df70.	2021-03-26	4.7	CVE-2021-29265 MISC MISC
linux -- linux_kernel	A flaw possibility of race condition and incorrect initialization of the process id was found in the Linux kernel child/parent process identification handling while filtering signal handlers. A local attacker is able to abuse this flaw to bypass checks to send any signal to a privileged process.	2021-03-26	4.4	CVE-2020-35508 MISC MISC
matrix -- synapse	Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.27.0, the password reset endpoint served via Synapse was vulnerable to cross-site scripting (XSS) attacks. The impact depends on the configuration of the domain that Synapse is deployed on, but may allow access to cookies and other browser data, CSRF vulnerabilities, and access to other resources served on the same domain or parent domains. This is fixed in version 1.27.0.	2021-03-26	4.3	CVE-2021-21332 MISC MISC MISC CONFIRM
mcafee -- epolicy_orchestrator	Unvalidated client-side URL redirect vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 10 could cause an authenticated ePO user to load an untrusted site in an ePO iframe which could steal information from the authenticated user.	2021-03-26	4.9	CVE-2021-23888 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mcafee -- epolicy_orchestrator	Information leak vulnerability in the Agent Handler of McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 10 allows an unauthenticated user to download McAfee product packages (specifically McAfee Agent) available in ePO repository and install them on their own machines to have it managed and then in turn get policy details from the ePO server. This can only happen when the ePO Agent Handler is installed in a Demilitarized Zone (DMZ) to service machines not connected to the network through a VPN.	2021-03-26	5.8	CVE-2021-23890 CONFIRM
microco -- bluemonday	bluemonday before 1.0.5 allows XSS because certain Go lowercasing converts an uppercase Cyrillic character, defeating a protection mechanism against the "script" string.	2021-03-27	4.3	CVE-2021-29272 MISC MISC
microfocus -- access_manager	Cross-Site scripting vulnerability in Micro Focus Access Manager product, affects all version prior to version 5.0. The vulnerability could cause configuration destruction.	2021-03-26	4.3	CVE-2020-25840 MISC
microfocus -- access_manager	Advance configuration exposing Information Leakage vulnerability in Micro Focus Access Manager product, affects all versions prior to version 5.0. The vulnerability could cause information leakage.	2021-03-26	5	CVE-2021-22506 MISC
mobileiron -- mobile\@work	The MobileIron agents through 2021-03-22 for Android and iOS contain a hardcoded encryption key, used to encrypt the submission of username/password details during the authentication process, as demonstrated by Mobile@Work (aka com.mobileiron). The key is in the com/mobileiron/common/utils/C4928m.java file.	2021-03-29	5	CVE-2020-35138 MISC MISC MISC
mobileiron -- mobile\@work	The MobileIron agents through 2021-03-22 for Android and iOS contain a hardcoded API key, used to communicate with the MobileIron SaaS discovery API, as demonstrated by Mobile@Work (aka com.mobileiron). The key is in com/mobileiron/registration/RegisterActivity.java and can be used for api/v1/gateway/customers/servers requests.	2021-03-29	4.3	CVE-2020-35137 MISC MISC MISC
netgear -- prosafe_network_management_system	This vulnerability allows remote attackers to disclose sensitive information and delete arbitrary files on affected installations of NETGEAR ProSAFE Network Management System 1.6.0.26. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the ConfigFileController class. When parsing the realName parameter, the process does not properly validate a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose sensitive information or to create a denial-of-service condition on the system. Was ZDI-CAN-12125.	2021-03-29	6.5	CVE-2021-27275 MISC MISC
netgear -- prosafe_network_management_system	This vulnerability allows remote attackers to delete arbitrary files on affected installations of NETGEAR ProSAFE Network Management System 1.6.0.26. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the MibController class. When parsing the realName parameter, the process does not properly validate a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-12122.	2021-03-29	5.5	CVE-2021-27276 MISC MISC
nic -- knot_resolver	A flaw was found in knot-resolver before version 2.3.0. Malformed DNS messages may cause denial of service.	2021-03-30	5	CVE-2018-1110 MISC MISC
nim-lang -- nim	Nimble is a package manager for the Nim programming language. In Nim release version before versions 1.2.10 and 1.4.4, Nimble doCmd is used in different places and can be leveraged to execute arbitrary commands. An attacker can craft a malicious entry in the packages.json package list to trigger code execution.	2021-03-26	6.8	CVE-2021-21372 MISC MISC MISC CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nim-lang -- nim	Nimble is a package manager for the Nim programming language. In Nim release versions before versions 1.2.10 and 1.4.4, "nimble refresh" fetches a list of Nimble packages over HTTPS without full verification of the SSL/TLS certificate due to the default setting of httpClient. An attacker able to perform MitM can deliver a modified package list containing malicious software packages. If the packages are installed and used the attack escalates to untrusted code execution.	2021-03-26	6.8	CVE-2021-21374 MISC MISC MISC CONFIRM
nim-lang -- nim	Nimble is a package manager for the Nim programming language. In Nim release versions before versions 1.2.10 and 1.4.4, "nimble refresh" fetches a list of Nimble packages over HTTPS by default. In case of error it falls back to a non-TLS URL http://irclogs.nim-lang.org/packages.json. An attacker able to perform MitM can deliver a modified package list containing malicious software packages. If the packages are installed and used the attack escalates to untrusted code execution.	2021-03-26	4.3	CVE-2021-21373 MISC MISC CONFIRM
parallels -- parallels_desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.0.1-48919. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-11924.	2021-03-29	4.6	CVE-2021-27243 N/A N/A
parallels -- parallels_desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.0.1-48919. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-11926.	2021-03-29	4.6	CVE-2021-27242 N/A N/A
portprocesses_project -- portprocesses	This affects the package portprocesses before 1.0.5. If (attacker-controlled) user input is given to the killProcess function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-03-31	6.5	CVE-2021-23348 MISC MISC MISC MISC
redhat -- 389_directory_server	When binding against a DN during authentication, the reply from 389-ds-base will be different whether the DN exists or not. This can be used by an unauthenticated attacker to check the existence of an entry in the LDAP database.	2021-03-26	5	CVE-2020-35518 MISC MISC MISC MISC
redhat -- resteasy	A flaw was found in RESTEasy in all versions of RESTEasy up to 4.6.0.Final. The endpoint class and method names are returned as part of the exception response when RESTEasy cannot convert one of the request URI path or query values to the matching JAX-RS resource method's parameter value. The highest threat from this vulnerability is to data confidentiality.	2021-03-26	5	CVE-2021-20289 MISC
redmine -- redmine	Redmine 4.1.x before 4.1.2 allows XSS because an issue's subject is mishandled in the auto complete tip.	2021-03-29	4.3	CVE-2021-29274 MISC MISC
remark42 -- remark42	remark42 before 1.6.1 allows XSS, as demonstrated by "Locator: Locator{URL:" followed by an XSS payload. This is related to backend/app/store/comment.go and backend/app/store/service/service.go.	2021-03-27	4.3	CVE-2021-29271 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rocket.chat -- rocket.chat	Rocket.Chat before 3.11, 3.10.5, 3.9.7, 3.8.8 is vulnerable to persistent cross-site scripting (XSS) using nested markdown tags allowing a remote attacker to inject arbitrary JavaScript in a message. This flaw leads to arbitrary file read and RCE on Rocket.Chat desktop app.	2021-03-26	4.3	CVE-2021-22886 MISC MISC MISC
rpm -- rpm	A flaw was found in RPM's signature check functionality when reading a package file. This flaw allows an attacker who can convince a victim to install a seemingly verifiable package, whose signature header was modified, to cause RPM database corruption and execute code. The highest threat from this vulnerability is to data integrity, confidentiality, and system availability.	2021-03-26	5.1	CVE-2021-20271 MISC MISC FEDORA FEDORA
sherlockim -- sherlockim	Sherlock SherlockIM through 2021-03-29 allows Cross Site Scripting (XSS) by leveraging the api/Files/Attachment URI to attack help-desk staff via the chatbot feature.	2021-03-29	4.3	CVE-2021-29267 MISC MISC
simple_college_project -- simple_college	Simple College Website 1.0 allows a user to conduct remote code execution via /alumni/admin/ajax.php?action=save_settings when uploading a malicious file using the image upload functionality, which is stored in /alumni/admin/assets/uploads/.	2021-03-31	6.5	CVE-2020-28173 MISC MISC MISC MISC
solarwinds -- orion_platform	The custom menu item options page in SolarWinds Orion Platform before 2020.2.5 allows Reverse Tabnabbing in the context of an administrator account.	2021-03-26	4.9	CVE-2021-3109 CONFIRM MISC
tableau -- tableau_server	Tableau Server fails to validate certain URLs that are embedded in emails sent to Tableau Server users.	2021-03-26	5.8	CVE-2021-1629 MISC
tp-link -- td-w9977_firmware	Unauthenticated stored cross-site scripting (XSS) exists in multiple TP-Link products including WIFI Routers (Wireless AC routers), Access Points, ADSL + DSL Gateways and Routers, which affects TD-W9977v1, TL-WA801NDv5, TL-WA801Nv6, TL-WA802Nv5, and Archer C3150v2 devices through the improper validation of the hostname. Some of the pages including dhcp.htm, networkMap.htm, dhcpClient.htm, qsEdit.htm, and qsReview.htm and use this vulnerable hostname function (setDefaultHostname()) without sanitization.	2021-03-26	4.3	CVE-2021-3275 MISC MISC FULLDISC MISC
wire -- wire	wire-server is an open-source back end for Wire, a secure collaboration platform. In wire-server from version 2021-02-16 and before version 2021-03-02, the client metadata of all users was exposed in the `GET /users/list-clients` endpoint. The endpoint could be used by any logged in user who could request client details of any other user (no connection required) as far as they can find their User ID. The exposed metadata included id, class, type, location, time, and cookie. A user on a Wire backend could use this endpoint to find registration time and location for each device for a given list of users. As a workaround, remove `/list-clients` from nginx config. This has been fixed in version 2021-03-02.	2021-03-26	4	CVE-2021-21396 MISC MISC CONFIRM
xerox -- altalink_b8045_firmware	Xerox AltaLink B80xx before 103.008.020.23120, C8030/C8035 before 103.001.020.23120, C8045/C8055 before 103.002.020.23120 and C8070 before 103.003.020.23120 provide the ability to set configuration attributes without administrative rights.	2021-03-29	5	CVE-2021-28669 CONFIRM
xerox -- altalink_b8045_firmware	Xerox AltaLink B8045/B8090 before 103.008.030.32000, C8030/C8035 before 103.001.030.32000, C8045/C8055 before 103.002.030.32000 and C8070 before 103.003.030.32000 allow unauthorized users, by leveraging the Scan To Mailbox feature, to delete arbitrary files from the disk.	2021-03-29	6.4	CVE-2021-28670 CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arubanetworks -- instant	A remote unauthorized disclosure of information vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.4.x: 6.4.4.8-4.2.4.18 and below; Aruba Instant 6.5.x: 6.5.4.18 and below; Aruba Instant 8.3.x: 8.3.0.14 and below; Aruba Instant 8.5.x: 8.5.0.10 and below; Aruba Instant 8.6.x: 8.6.0.5 and below; Aruba Instant 8.7.x: 8.7.0.0 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.	2021-03-30	3.3	CVE-2021-25145 MISC
avast -- premium_security	This vulnerability allows local attackers to delete arbitrary directories on affected installations of Avast Premium Security 20.8.2429 (Build 20.8.5653.561). An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the AvastSvc.exe module. By creating a directory junction, an attacker can abuse the service to delete a directory. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-12082.	2021-03-29	3.6	CVE-2021-27241 N/A
basercms -- basercms	Improper neutralization of JavaScript input in the page editing function of baserCMS versions prior to 4.4.5 allows remote authenticated attackers to inject an arbitrary script via unspecified vectors.	2021-03-26	3.5	CVE-2021-20681 MISC MISC
basercms -- basercms	Improper neutralization of JavaScript input in the blog article editing function of baserCMS versions prior to 4.4.5 allows remote authenticated attackers to inject an arbitrary script via unspecified vectors.	2021-03-26	3.5	CVE-2021-20683 MISC MISC
ca -- ehealth_performance_manager	** UNSUPPORTED WHEN ASSIGNED ** CA eHealth Performance Manager through 6.3.2.12 is affected by Cross Site Scripting (XSS). The impact is: An authenticated remote user is able to inject arbitrary web script or HTML due to incorrect sanitization of user-supplied data and perform a Reflected Cross-Site Scripting attack against the platform users. The affected endpoints are: cgi/nhWeb with the parameter report, aviewbin/filtermibobjects.pl with the parameter namefilter, and aviewbin/query.pl with the parameters System, SystemText, Group, and GroupText. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-03-26	3.5	CVE-2021-28247 MISC
gitlab -- gitlab	An information disclosure issue in GitLab starting from version 12.8 allowed a user with access to the server logs to see sensitive information that wasn't properly redacted.	2021-03-26	2.1	CVE-2021-22184 CONFIRM MISC
gitlab -- gitlab	In all versions of GitLab starting from 13.7, marshalled session keys were being stored in Redis.	2021-03-26	2.1	CVE-2021-22194 CONFIRM MISC
gnu -- binutils	There is an open race window when writing output in the following utilities in GNU binutils version 2.35 and earlier:ar, objcopy, strip, ranlib. When these utilities are run as a privileged user (presumably as part of a script updating binaries across different users), an unprivileged user can trick these utilities into getting ownership of arbitrary files through a symlink.	2021-03-26	3.3	CVE-2021-20197 MISC MISC
google -- android	An improper access control vulnerability in sec_log file prior to SMR MAR-2021 Release 1 exposes sensitive kernel information to userspace.	2021-03-26	2.1	CVE-2021-25369 MISC CONFIRM
hpe -- unified_data_management	A security vulnerability in HPE Unified Data Management (UDM) could allow the local disclosure of privileged information (CWE-321: Use of Hard-coded Cryptographic Key in a product). HPE has provided updates to versions 1.2009.0 and 1.2101.0 of HPE Unified Data	2021-03-30	2.1	CVE-2021-26579 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Management (UDM). Version 1.2103.0 of HPE Unified Data Management (UDM) removes all hard-coded cryptographic keys.			
ibm -- engineering_insights	IBM Jazz Foundation Products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198182.	2021-03-30	3.5	CVE-2021-20503 XF CONFIRM
ibm -- engineering_insights	IBM Jazz Foundation Products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196623.	2021-03-30	3.5	CVE-2021-20447 XF CONFIRM
ibm -- engineering_insights	IBM Jazz Foundation Products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194710.	2021-03-30	3.5	CVE-2021-20352 XF CONFIRM
ibm -- engineering_insights	IBM Jazz Foundation Products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198231.	2021-03-30	3.5	CVE-2021-20504 XF CONFIRM
ibm -- engineering_insights	IBM Jazz Foundation Products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198231.	2021-03-30	3.5	CVE-2021-20506 XF CONFIRM
ibm -- engineering_insights	IBM Jazz Foundation Products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198572.	2021-03-30	3.5	CVE-2021-20520 XF CONFIRM
ibm -- engineering_insights	IBM Jazz Foundation Products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198437.	2021-03-30	3.5	CVE-2021-20518 XF CONFIRM
ibm -- urbancode_deploy	IBM UrbanCode Deploy (UCD) 7.0.3.0, 7.0.4.0, 7.0.5.3, 7.0.5.4, 7.1.0.0, 7.1.1.0, 7.1.1.1, and 7.1.1.2, stores keystore passwords in plain in plain text after a manuel edit, which can be read by a local user. IBM X-Force ID: 191944.	2021-03-30	2.1	CVE-2020-4944 XF CONFIRM
ibm -- urbancode_deploy	IBM UrbanCode Deploy (UCD) 6.2.7.9, 7.0.5.4, and 7.1.1.1 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 190908.	2021-03-30	2.1	CVE-2020-4884 XF CONFIRM
jenkins -- build_with_parameters	Jenkins Build With Parameters Plugin 1.5 and earlier does not escape parameter names and descriptions, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	2021-03-30	3.5	CVE-2021-21628 MLIST CONFIRM
jenkins -- extra_columns	Jenkins Extra Columns Plugin 1.22 and earlier does not escape parameter values in the build parameters column, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	2021-03-30	3.5	CVE-2021-21630 MLIST CONFIRM
matrix -- synapse	Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.27.0, the notification emails sent for notifications for missed messages or for an expiring account are subject to HTML injection. In the case of the notification for missed messages, this could allow an attacker to insert forged content into	2021-03-26	2.6	CVE-2021-21333 MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the email. The account expiry feature is not enabled by default and the HTML injection is not controllable by an attacker. This is fixed in version 1.27.0.			MISC CONFIRM
mblog_project -- mblog	Cross Site Scripting (XSS) vulnerability in mblog 3.5 via the post content field to /post/editing.	2021-04-01	3.5	CVE-2020-19618 MISC
mblog_project -- mblog	Cross Site Scripting (XSS) vulnerability in mblog 3.5 via the nickname field to /settings/profile.	2021-04-01	3.5	CVE-2020-19617 MISC
mblog_project -- mblog	Cross Site Scripting (XSS) vulnerability in mblog 3.5 via the post header field to /post/editing.	2021-04-01	3.5	CVE-2020-19616 MISC
mblog_project -- mblog	Cross Site Scripting (XSS) vulnerability in mblog 3.5 via the signature field to /settings/profile.	2021-04-01	3.5	CVE-2020-19619 MISC
mcafee -- epolicy_orchestrator	Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 10 allows ePO administrators to inject arbitrary web script or HTML via multiple parameters where the administrator's entries were not correctly sanitized.	2021-03-26	3.5	CVE-2021-23889 CONFIRM
microseven -- mym71080i-b_firmware	MicroSeven MYM71080i-B 2.0.5 through 2.0.20 devices send admin credentials in cleartext to pnp.microseven.com TCP port 7007. An attacker on the same network as the device can capture these credentials.	2021-03-26	2.9	CVE-2021-29255 MISC MISC
necplatforms -- univerge_aspire_wx_firmware	UNIVERGE Aspire series PBX (UNIVERGE Aspire WX from 1.00 to 3.51, UNIVERGE Aspire UX from 1.00 to 9.70, UNIVERGE SV9100 from 1.00 to 10.70, and SL2100 from 1.00 to 3.00) allows a remote authenticated attacker to cause system down and a denial of service (DoS) condition by sending a specially crafted command.	2021-03-26	3.5	CVE-2021-20677 MISC MISC
parallels -- parallels_desktop	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 16.0.1-48919. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-11925.	2021-03-29	2.1	CVE-2021-27244 N/A N/A
prestashop -- prestashop	PrestaShop is a fully scalable open source e-commerce solution. In PrestaShop before version 1.7.7.3, an attacker can inject HTML when the Grid Column Type DataColumn is badly used. The problem is fixed in 1.7.7.3	2021-03-30	3.5	CVE-2021-21398 MISC MISC CONFIRM
seeyon -- g6_government_collaborative_system	Cross-Site Scripting (XSS) vulnerability in Zhiyuan G6 Government Collaboration System V6.1SP1, via the 'method' parameter to 'seeyon/hrSalary.do'.	2021-03-30	3.5	CVE-2020-20545 MISC MISC
solarwinds -- orion_platform	SolarWinds Orion Platform before 2020.2.5 allows stored XSS attacks by an administrator on the Customize View page.	2021-03-26	3.5	CVE-2020-35856 CONFIRM MISC