BULLETIN (SB20-188)
VULNERABILITY SUMMARY FOR THE WEEK OF
29TH JUNE, 2020

Bulletin (SB20-188)
Vulnerability Summary for the Week of June 29, 2020

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
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9566 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9564 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9562 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9569 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9568 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9565 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9567 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9563 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9559 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9560 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9556 CONFIRM

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have a stack-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9555 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9554 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9561 CONFIRM
adobe -- character_animator	Adobe Character Animator versions 3.2 and earlier have a buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9586 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9589 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9590 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9620 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9621 CONFIRM
adobe -- illustrator	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9573 CONFIRM
adobe -- illustrator	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9574 CONFIRM
adobe -- illustrator	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9572 CONFIRM
adobe -- illustrator	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9571 CONFIRM

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- illustrator	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9570 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a defense-in-depth security mitigation vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9585 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9576 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9582 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9583 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9580 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	10	CVE-2020-9631 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9578 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a business logic error vulnerability. Successful exploitation could lead to privilege escalation.	2020-06-26	7.5	CVE-2020-9630 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	10	CVE-2020-9632 CONFIRM

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9579 CONFIRM
draytek -- multiple_devices	On DrayTek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1, cgi-bin/mainfunction.cgi/cvmcfgupload allows remote command execution via shell metacharacters in a filename when the text/x-python-script content type is used, a different issue than CVE-2020-14472.	2020-06-30	7.5	CVE-2020-15415 MISC MISC
f5 -- big-ip	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.	2020-07-01	10	CVE-2020-5902 MISC
mk-auth -- mk-auth	An issue was discovered in MK-AUTH 19.01. The web login functionality allows an attacker to bypass authentication and gain client privileges via SQL injection in central/executar_login.php.	2020-06-29	7.5	CVE-2020-14068 MISC MISC
mk-auth -- mk-auth	An issue was discovered in MK-AUTH 19.01. It allows command execution as root via shell metacharacters to /auth admin scripts.	2020-06-29	10	CVE-2020-14072 MISC MISC
mk-auth -- mk-auth	An issue was discovered in MK-AUTH 19.01. There is authentication bypass in the web login functionality because guessable credentials to admin/executar_login.php result in admin access.	2020-06-29	10	CVE-2020-14070 MISC MISC
opensis -- opensis	openSIS through 7.4 allows SQL Injection.	2020-07-01	7.5	CVE-2020-13381 MISC MISC
opensis -- opensis	openSIS before 7.4 allows SQL Injection.	2020-07-01	7.5	CVE-2020-13380 CONFIRM MISC
prestashop -- prestashop	In PrestaShop from version 1.6.0.1 and before version 1.7.6.6, the dashboard allows rewriting all configuration variables. The problem is fixed in 1.7.6.6	2020-07-02	7.5	CVE-2020-15082 MISC CONFIRM
prestashop -- prestashop	In PrestaShop from version 1.5.0.0 and before version 1.7.7.6, the authentication system is malformed and an	2020-07-02	10	CVE-2020-4074

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker is able to forge requests and execute admin commands. The problem is fixed in 1.7.7.6.			MISC CONFIRM
sqlite -- sqlite	In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transitive properties for constant propagation.	2020-06-27	7.5	CVE-2020-15358 MISC MISC MISC
stash -- stash	Stash 1.0.3 allows SQL Injection via the downloadmp3.php download parameter.	2020-06-26	7.5	CVE-2020-15311 MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has the axiros password for the root account.	2020-06-29	7.5	CVE-2020-15320 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a world-readable axess/opt/axXMPPHandler/config/xmpp_config.py file that stores hardcoded credentials.	2020-06-29	7.5	CVE-2020-15324 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- after_effects	Adobe After Effects versions 17.0.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2020-06-26	4.3	CVE-2020-3809 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9553 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9557 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9558 CONFIRM
adobe -- coldfusion	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have an improper access control vulnerability. Successful exploitation could lead to system file structure disclosure.	2020-06-26	4.3	CVE-2020-3796 CONFIRM
adobe -- coldfusion	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have an insufficient input validation vulnerability. Successful exploitation could lead to application-level denial-of-service (dos).	2020-06-26	4.3	CVE-2020-3767 CONFIRM
adobe -- coldfusion	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have a dll search-order hijacking vulnerability. Successful exploitation could lead to privilege escalation.	2020-06-26	4.4	CVE-2020-3768 CONFIRM
adobe -- digital_editions	Adobe Digital Editions versions 4.5.11.187212 and below have a file enumeration (host or local network) vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-3798 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	5	CVE-2020-9627 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9622 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9624 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	5	CVE-2020-9628 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9626 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	5	CVE-2020-9625 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9629 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	5	CVE-2020-9623 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a defense-in-depth security mitigation vulnerability. Successful exploitation could lead to unauthorized access to admin panel.	2020-06-26	5	CVE-2020-9591 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have an observable timing discrepancy vulnerability. Successful exploitation could lead to signature verification bypass.	2020-06-26	6.5	CVE-2020-9588 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure .	2020-06-26	4.3	CVE-2020-9577 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2020-06-26	4.3	CVE-2020-9581 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have an authorization bypass vulnerability. Successful exploitation could lead to potentially unauthorized product discounts.	2020-06-26	5	CVE-2020-9587 CONFIRM
adobe -- premiere_pro	Adobe Premiere Pro versions 14.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9616 CONFIRM
adobe -- premiere_rush	Adobe Premiere Rush versions 1.5.8 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9617 CONFIRM
apache -- tomcat	A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat 10.0.0-M1 to 10.0.0-M5, 9.0.0.M1 to 9.0.35 and 8.5.0 to 8.5.55 could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive.	2020-06-26	5	CVE-2020-11996 MLIST CONFIRM MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST
cybozu -- garoon	Path traversal vulnerability in Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to obtain unintended information via unspecified vectors.	2020-06-30	4	CVE-2020-5581 MISC MISC
cybozu -- garoon	Path traversal vulnerability in Cybozu Garoon 5.0.0 to 5.0.1 allows attacker with administrator rights to obtain unintended information via unspecified vectors.	2020-06-30	4	CVE-2020-5588 MISC MISC
docker -- docker_desktop	com.docker.vmnetd in Docker Desktop 2.3.0.3 allows privilege escalation because of a lack of client verification.	2020-06-27	4.6	CVE-2020-15360 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- api_connect	IBM API Connect V2018.4.1.0 through 2018.4.1.11 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 181324.	2020-06-29	5	CVE-2020-4452 XF CONFIRM
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.6.1.1 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 170961.	2020-06-26	6.5	CVE-2019-4650 XF CONFIRM
ibm -- security_identity_manager_virtual_appliance	IBM Security Identity Manager Virtual Appliance 7.0.2 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 172015.	2020-07-01	4	CVE-2019-4705 XF CONFIRM
ibm -- security_identity_manager_virtual_appliance	IBM Security Identity Manager Virtual Appliance 7.0.2 writes information to log files which can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information. IBM X-Force ID: 172016.	2020-07-01	4	CVE-2019-4706 XF CONFIRM
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow an attacker to obtain sensitive information due to insecure communications being used between the application and server. IBM X-Force ID: 183935.	2020-06-26	4.3	CVE-2020-4565 XF CONFIRM
jiangmin -- jiangmin_antivirus	In Jiangmin Antivirus 16.0.13.129, the driver file (KVFG.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x220440.	2020-06-26	4.9	CVE-2020-14955 MISC
mattermost -- mattermost_mobile_app	An issue was discovered in Mattermost Mobile Apps before 1.31.2 on iOS. Unintended third-party servers could sometimes obtain authorization tokens, aka MMSA-2020-0022.	2020-06-26	5	CVE-2020-13891 CONFIRM
mediaarea -- mediainfo	In MediaInfoLib in MediaArea MediaInfo 20.03, there is a stack-based buffer over-read in Streams_Fill_PerStream in Multiple/File_MpegPs.cpp (aka an off-by-one during MpegPs parsing).	2020-06-30	6.8	CVE-2020-15395 MISC MISC
mk-auth -- mk-auth	IBM Security Identity Manager Virtual Appliance 7.0.2 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 172014.	2020-07-01	4.3	CVE-2019-4704 XF CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mk-auth -- mk-auth	An issue was discovered in MK-AUTH 19.01. XSS vulnerabilities in admin and client scripts allow an attacker to execute arbitrary JavaScript code.	2020-06-29	4.3	CVE-2020-14071 MISC MISC
mk-auth -- mk-auth	An issue was discovered in MK-AUTH 19.01. There are SQL injection issues in mkt/ PHP scripts, as demonstrated by arp.php, dhcp.php, hotspot.php, ip.php, pgaviso.php, pgcorte.php, pppoe.php, queues.php, and wifi.php.	2020-06-29	4.6	CVE-2020-14069 MISC MISC
nedi_consulting -- nedi	NeDi 1.9C is vulnerable to reflected cross-site scripting. The Other-Converter.php file improperly validates user input. An attacker can exploit this vulnerability by crafting arbitrary JavaScript in the txt GET parameter.	2020-06-26	4.3	CVE-2020-15016 MISC
nedi_consulting -- nedi	NeDi 1.9C is vulnerable to reflected cross-site scripting. The Devices-Config.php file improperly validates user input. An attacker can exploit this vulnerability by crafting arbitrary JavaScript in the sta GET parameter.	2020-06-26	4.3	CVE-2020-15017 MISC
opensis -- opensis	openSIS through 7.4 allows Directory Traversal.	2020-07-01	5	CVE-2020-13383 MISC MISC
opensis -- opensis	openSIS through 7.4 has Incorrect Access Control.	2020-07-01	6.4	CVE-2020-13382 MISC MISC
prestashop -- prestashop	In PrestaShop from version 1.7.0.0 and before version 1.7.6.6, if a target sends a corrupted file, it leads to a reflected XSS. The problem is fixed in 1.7.6.6	2020-07-02	4.3	CVE-2020-15083 MISC CONFIRM
prestashop -- prestashop	In PrestaShop from version 1.5.0.0 and before 1.7.6.6, there is information exposure in the upload directory. The problem is fixed in version 1.7.6.6. A possible workaround is to add an empty index.php file in the upload directory.	2020-07-02	5	CVE-2020-15081 MISC CONFIRM
wordpress -- wordpress	The Nexos theme through 1.7 for WordPress allows top-map/?search_location= reflected XSS.	2020-06-28	4.3	CVE-2020-15364 MISC MISC
wordpress -- wordpress	The Nexos theme through 1.7 for WordPress allows side-map/?search_order= SQL Injection.	2020-06-28	5	CVE-2020-15363 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded RSA SSH key for the root account within the /opt/mysql chroot directory tree.	2020-06-29	4.3	CVE-2020-15319 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded RSA SSH key for the root account.	2020-06-29	4.3	CVE-2020-15314 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded ECDSA SSH key for the root account.	2020-06-29	4.3	CVE-2020-15313 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded DSA SSH key for the root account.	2020-06-29	4.3	CVE-2020-15312 MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2020-06-26	3.5	CVE-2020-9584 CONFIRM
adobe -- magento	Form Builder 2.1.0 for Magento has multiple XSS issues that can be exploited against Magento 2 admin accounts via the Current_url or email field, or the User-Agent HTTP header.	2020-06-29	3.5	CVE-2020-13423 MISC MISC MISC
atlassian -- jira_server_and_data_center	The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a vnd.wap.xhtml+xml content type.	2020-07-01	3.5	CVE-2020-4024 MISC
avast -- avast_antivirus	An elevation of privilege vulnerability exists in Avast Free Antivirus and AVG AntiVirus Free before 20.4 due to improperly handling hard links. The vulnerability allows local users to take control of arbitrary files.	2020-06-29	2.1	CVE-2020-13657 CONFIRM CONFIRM
cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 5.0.0 to 5.0.1 allows attacker with administrator rights to inject an arbitrary script via unspecified vectors.	2020-06-30	3.5	CVE-2020-5585 MISC MISC
cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 4.10.3 to 5.0.1 allows attacker with administrator rights to inject an arbitrary script via unspecified vectors.	2020-06-30	3.5	CVE-2020-5586 MISC MISC
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.6.0.10 and 7.6.1.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 175121.	2020-06-26	3.5	CVE-2020-4223 XF CONFIRM
ibm -- security_identity_manager_virtual_appliance	IBM Security Identity Manager Virtual Appliance 7.0.2 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 171512.	2020-07-01	2.1	CVE-2019-4676 XF CONFIRM
linux -- linux_kernel	In the Linux kernel through 5.7.6, usbtest_disconnect in drivers/usb/misc/usbtest.c has a memory leak, aka CID-28ebeb8db770.	2020-06-29	2.1	CVE-2020-15393 MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openexr -- openexr	An issue was discovered in OpenEXR before 2.5.2. An invalid tiled input file could cause invalid memory access in TiledInputFile::TiledInputFile() in IlmImf/ImfTiledInputFile.cpp, as demonstrated by a NULL pointer dereference.	2020-06-26	2.1	CVE-2020-15304 MISC MISC MISC MISC
openexr -- openexr	An issue was discovered in OpenEXR before 2.5.2. Invalid input could cause a use-after-free in DeepScanLineInputFile::DeepScanLineInputFile() in IlmImf/ImfDeepScanLineInputFile.cpp.	2020-06-26	2.1	CVE-2020-15305 MISC MISC MISC MISC
openexr -- openexr	An issue was discovered in OpenEXR before v2.5.2. Invalid chunkCount attributes could cause a heap buffer overflow in getChunkOffsetTableSize() in IlmImf/ImfMisc.cpp.	2020-06-26	2.1	CVE-2020-15306 MISC MISC MISC MISC
prestashop -- prestashop	In PrestaShop from version 1.5.3.0 and before version 1.7.7.6, there is a stored XSS when using the name of a quick access item. The problem is fixed in 1.7.7.6.	2020-07-02	3.5	CVE-2020-11074 MISC CONFIRM