BULLETIN (SB19-308)

VULNERABILITY SUMMARY FOR THE WEEK OF OCTOBER 28, 2019

Bulletin (SB19-308)
Vulnerability Summary for the Week of October 28, 2019

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 -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-10-25	7.5	CVE-2019-8088 CONFIRM
apache -- thrift	In Apache Thrift all versions up to and including 0.12.0, a server or client may run into an endless loop when feed with specific input data. Because the issue had already been partially fixed in version 0.11.0, depending on the installed version it affects only certain language bindings.	2019-10-29	7.8	CVE-2019-0205 MISC
bitlbee -- bitlbee	Bitlbee does not drop extra group privileges correctly in unix.c	2019-10-29	7.5	CVE-2012-1187
cisco -- video_communications_server	Cisco Video Communications Server (VCS) before X7.0.3 contains a command injection vulnerability which allows remote, authenticated attackers to execute arbitrary commands.	2019-10-29	9	CVE-2011-2538 CONFIRM
codesys -- eni_server	CODESYS V2.3 ENI server up to V3.2.2.24 has a Buffer Overflow.	2019-10-25	7.5	CVE-2019-16265 CONFIRM MISC
d-link -- dir-865	D-Link DIR-865L has PHP File Inclusion in the router xml file.	2019-10-25	7.5	CVE-2013-4857 MISC MISC
d-link -- dir-865l_devices	D-Link DIR-865L has SMB Symlink Traversal due to misconfiguration in the SMB service allowing symbolic links to be created to locations outside of the Samba share.	2019-10-25	7.9	CVE-2013-4855 MISC MISC MISC
debian_project -- qtparted	qtparted has insecure library loading which may allow arbitrary code execution	2019-10-29	7.5	CVE-2010-3375 DEBIAN MISC MISC
google -- chrome	browser/extensions/api/dial/dial_registry.cc in Google Chrome before 54.0.2840.98 on macOS, before 54.0.2840.99 on Windows, and before 54.0.2840.100 on Linux neglects to copy a device ID before an erase() call, which causes the erase operation to access data that that erase operation will destroy.	2019-10-25	7.5	CVE-2016-5202
hot-world -- repetier-server	A directory traversal vulnerability was discovered in RepetierServer.exe in Repetier-Server 0.8 through 0.91 that allows for the creation of a user controlled XML file at an unintended location. When this is combined with CVE-2019-14451, an attacker can upload an "external command"	2019-10-28	10	CVE-2019-14450 CONFIRM MISC

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configuration as a printer configuration, and achieve remote code execution. After exploitation, loading of the external command configuration is dependent on a system reboot or service restart.			
hot-world -- repetier-server	RepetierServer.exe in Repetier-Server 0.8 through 0.91 does not properly validate the XML data structure provided when uploading a new printer configuration. When this is combined with CVE-2019-14450, an attacker can upload an "external command" configuration as a printer configuration, and achieve remote code execution. After exploitation, loading of the external command configuration is dependent on a system reboot or service restart.	2019-10-25	10	CVE-2019-14451 CONFIRM MISC
intrasrv -- intrasrv	A remote SEH buffer overflow has been discovered in IntraSrv 1.0 (2007-06-03). An attacker may send a crafted HTTP GET or HEAD request that can result in a compromise of the hosting system.	2019-10-28	10	CVE-2019-17181 MISC MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2019.1.4, insecure Java Deserialization could potentially allow remote code execution.	2019-10-31	7.5	CVE-2019-18364 CONFIRM
k7_computing -- antivirus_premium_and_total_security_and_ultimate_security	In K7 Antivirus Premium 16.0.xxx through 16.0.0120; K7 Total Security 16.0.xxx through 16.0.0120; and K7 Ultimate Security 16.0.xxx through 16.0.0120, the module K7TSHlpr.dll improperly validates the administrative privileges of the user, allowing arbitrary registry writes in the K7AVOptn.dll module to facilitate escalation of privileges via inter-process communication with a service process.	2019-10-28	7.5	CVE-2019-16897 MISC
labf -- nfsaxe_ftp_client	Buffer overflow in LabF nfsAxe FTP client 3.7 allows an attacker to execute code remotely.	2019-10-25	7.5	CVE-2017-14742 EXPLOIT-DB
linksys -- ea6500_router	Linksys EA6500 has SMB Symlink Traversal allowing symbolic links to be created to locations outside of the Samba share.	2019-10-25	10	CVE-2013-4658 MISC MISC MISC
medoo -- medoo	columnQuote in medoo before 1.7.5 allows remote attackers to perform a SQL Injection due to improper escaping.	2019-10-30	7.5	CVE-2019-10762 MISC MISC
mikrotik -- routeros	RouterOS 6.45.6 Stable, RouterOS 6.44.5 Long-term, and below insufficiently validate where upgrade packages are download from when using the autoupgrade feature. Therefore, a remote attacker can trick the router into "upgrading" to an older version of RouterOS and possibly reseting all the system's usernames and passwords.	2019-10-29	8.5	CVE-2019-3977 MISC

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 have a buffer overflow in a web application via a long username or password.	2019-10-25	7.5	CVE-2016-2356
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 allow remote attackers to bypass authentication and access a protected resource by simultaneously making a request for the unprotected vb.htm resource.	2019-10-25	7.5	CVE-2016-2359
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Undocumented hard-coded user passwords for root, ineaadmin, mitsadmin, and maint could allow an attacker to gain unauthorised access to the RTU. (Also, the accounts ineaadmin and mitsadmin are able to escalate privileges to root without supplying a password due to insecure entries in /etc/sudoers on the RTU.)	2019-10-28	10	CVE-2019-14930 MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. An unauthenticated remote OS Command Injection vulnerability allows an attacker to execute arbitrary commands on the RTU due to the passing of unsafe user supplied data to the RTU's system shell. Functionality in mobile.php provides users with the ability to ping sites or IP addresses via Mobile Connection Test. When the Mobile Connection Test is submitted, action.php is called to execute the test. An attacker can use a shell command separator (;) in the host variable to execute operating system commands upon submitting the test data.	2019-10-28	10	CVE-2019-14931 MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Hard-coded SSH keys allow an attacker to gain unauthorised access or disclose encrypted data on the RTU due to the keys not being regenerated on initial installation or with firmware updates. In other words, these devices use private-key values in /etc/ssh/ssh_host_rsa_key, /etc/ssh/ssh_host_ecdsa_key, and /etc/ssh/ssh_host_dsa_key files that are publicly available from the vendor web sites.	2019-10-28	7.5	CVE-2019-14926 MISC MISC
philips -- intellispace_perinatal	In IntelliSpace Perinatal, Versions K and prior, a vulnerability within the IntelliSpace Perinatal application environment could enable an unauthorized attacker with physical access to a locked application screen, or an authorized remote desktop session host application user to break-out from the containment of the application and access unauthorized resources from the Windows operating system as the limited-access Windows user. Due to potential Windows vulnerabilities, it may be possible for additional attack methods to be used to escalate privileges on the operating system.	2019-10-25	7.2	CVE-2019-13546 MISC
php -- php	In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.	2019-10-28	7.5	CVE-2019-11043 REDHAT REDHAT REDHAT REDHAT CONFIRM

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC FEDORA FEDORA FEDORA CONFIRM CONFIRM UBUNTU UBUNTU DEBIAN DEBIAN
pixelpost -- pixelpost	pixelpost 1.7.1 has SQL injection	2019-10-28	7.5	CVE-2009-4899 MISC DEBIAN MISC
rconfig -- rconfig	An issue was discovered in rConfig 3.9.2. An attacker can directly execute system commands by sending a GET request to search.crud.php because the catCommand parameter is passed to the exec function without filtering, which can lead to command execution.	2019-10-28	9	CVE-2019-16663 MISC MISC MISC MISC MISC
rconfig -- rconfig	An issue was discovered in rConfig 3.9.2. An attacker can directly execute system commands by sending a GET request to ajaxServerSettingsChk.php because the rootUname parameter is passed to the exec function without filtering, which can lead to command execution.	2019-10-28	10	CVE-2019-16662 MISC MISC MISC MISC MISC MISC
rittal -- rittal_chiller_sk_3232_series	Rittal Chiller SK 3232-Series web interface as built upon Carel pCOWeb firmware A1.5.3 ? B1.2.4. The authentication mechanism on affected systems is configured using hard-coded credentials. These credentials could allow attackers to influence the primary operations of the affected systems, namely turning the cooling unit on and off and setting the temperature set point.	2019-10-25	10	CVE-2019-13553 FULLDISC MISC
sequelize -- sequelize	Sequelize all versions prior to 3.35.1, 4.44.3, and 5.8.11 are vulnerable to SQL Injection due to JSON path keys not being properly escaped for the MySQL/MariaDB dialects.	2019-10-29	7.5	CVE-2019-10748 MISC MISC MISC
sequelize -- sequelize	sequelize before version 3.35.1 allows attackers to perform a SQL Injection due to the JSON path keys not being properly sanitized in the Postgres dialect.	2019-10-29	7.5	CVE-2019-10749 MISC MISC

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
snoopy -- snoopy e	Snoopy before 2.0.0 has a security hole in exec cURL	2019-10-28	7.5	CVE-2002-2444 MISC DEBIAN MISC
sugarcrm -- sugarcrm	SugarCRM CE <= 6.3.1 contains scripts that use "unserialize()" with user controlled input which allows remote attackers to execute arbitrary PHP code.	2019-10-29	7.5	CVE-2012-0694 MISC MISC EXPLOIT-DB
tightvnc_software -- tightvnc	TightVNC code version 1.3.10 contains global buffer overflow in HandleCoRREBBP macro function, which can potentially result code execution. This attack appear to be exploitable via network connectivity.	2019-10-29	7.5	CVE-2019-8287 MLIST
tightvnc_software -- tightvnc	TightVNC code version 1.3.10 contains heap buffer overflow in InitialiseRFBConnection function, which can potentially result code execution. This attack appear to be exploitable via network connectivity.	2019-10-29	7.5	CVE-2019-15679 MLIST
tightvnc_software -- tightvnc	TightVNC code version 1.3.10 contains heap buffer overflow in rfbServerCutText handler, which can potentially result code execution.. This attack appear to be exploitable via network connectivity.	2019-10-29	7.5	CVE-2019-15678 MLIST
tiki_wiki -- cms_groupware	Tiki Wiki CMS Groupware 5.2 has Local File Inclusion	2019-10-28	7.5	CVE-2010-4239 MISC MISC MISC MISC
tp-link -- tl-wdr4300_devices	TP-Link TL-WDR4300 version 3.13.31 has multiple CSRF vulnerabilities.	2019-10-25	9.3	CVE-2013-4848 MISC MISC MISC MISC MISC
transmission -- transmission	Transmission before 1.92 allows an attacker to cause a denial of service (crash) or possibly have other unspecified impact via a large number of tr arguments in a magnet link.	2019-10-30	7.5	CVE-2010-0748 MISC CONFIRM MISC CONFIRM MLIST
youphptube -- youphptube	A command injection have been found in YouPHPTube Encoder. A successful attack could allow an attacker to compromise the server. Exploitable unauthenticated command injections exist in YouPHPTube	2019-10-25	7.5	CVE-2019-5127 MISC

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Encoder 2.3 a plugin for providing encoder functionality in YouPHPTube. The parameter base64Url in /objects/getImage.php is vulnerable to a command injection attack.			
youphptube -- youphptube	A command injection have been found in YouPHPTube Encoder. A successful attack could allow an attacker to compromise the server. Exploitable unauthenticated command injections exist in YouPHPTube Encoder 2.3 a plugin for providing encoder functionality in YouPHPTube. The parameter base64Url in /objects/getImageMP4.php is vulnerable to a command injection attack.	2019-10-25	7.5	CVE-2019-5128 MISC
youphptube -- youphptube	A command injection have been found in YouPHPTube Encoder. A successful attack could allow an attacker to compromise the server. Exploitable unauthenticated command injections exist in YouPHPTube Encoder 2.3 a plugin for providing encoder functionality in YouPHPTube. The parameter base64Url in /objects/getSpiritsFromVideo.php is vulnerable to a command injection attack.	2019-10-25	7.5	CVE-2019-5129 MISC
ytnef -- ytnef	ytnef has directory traversal	2019-10-29	7.5	CVE-2009-3887 MISC MISC MISC MISC MISC
zend_framework -- zend_framework	Zend Framework before 2.2.10 and 2.3.x before 2.3.5 has Potential SQL injection in PostgreSQL Zend\Db adapter.	2019-10-25	7.5	CVE-2015-0270 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a xml external entity injection vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	5	CVE-2019-8087 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4 and 6.3 have a cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	4.3	CVE-2019-8083 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a reflected cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	4.3	CVE-2019-8084 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a reflected cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	4.3	CVE-2019-8085 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.4, 6.3 and 6.2 have a cross-site request forgery vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	4.3	CVE-2019-8234 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have an authentication bypass vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	5	CVE-2019-8081 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.4, 6.3 and 6.2 have a xml external entity injection vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	5	CVE-2019-8082 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a xml external entity injection vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	5	CVE-2019-8086 CONFIRM
apache -- hadoop	Hadoop 1.0.3 contains a symlink vulnerability.	2019-10-29	5	CVE-2012-2945 MISC MISC
apache -- thrift	In Apache Thrift 0.9.3 to 0.12.0, a server implemented in Go using TJSONProtocol or TSimpleJSONProtocol may panic when feed with invalid input data.	2019-10-29	5	CVE-2019-0210 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows directory traversal by issuing a special HTTP POST request with ../ characters. This could lead to create malicious HTML file, because they can inject a content with crafted template. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	4.3	CVE-2019-17324 MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows remote attacker to upload arbitrary local file via the ActiveX method in RexViewerCtrl30.ocx. That could lead to disclosure of sensitive information. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	4.3	CVE-2019-17325 MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows remote attacker to arbitrary file deletion by issuing a HTTP GET request with a specially crafted parameter. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	5.8	CVE-2019-17326 MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows arbitrary file creation via a POST request with the parameter set to the file path to be written. This can be an executable file that is written to in the arbitrary directory. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	4.3	CVE-2019-17322 MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version have an information disclosure issue. When requesting web page associated with session, could leak username via session file path of HTTP response data. No authentication is required.	2019-10-30	5	CVE-2019-17321 MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows arbitrary file creation and execution via report print function of rexpert viewer with modified XML document. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	6.8	CVE-2019-17323 MISC
corehr -- core_portal	CoreHR Core Portal before 27.0.7 allows stored XSS.	2019-10-25	4.3	CVE-2019-18221 MISC MISC
debian_project -- mercurial	Mercurial before 1.6.4 fails to verify the Common Name field of SSL certificates which allows remote attackers who acquire a certificate signed by a Certificate Authority to perform a man-in-the-middle attack.	2019-10-29	4.3	CVE-2010-4237 MISC CONFIRM CONFIRM MISC
debian_project -- pootle	pootle 2.0.5 has XSS via 'match_names' parameter	2019-10-28	4.3	CVE-2010-4245 MISC DEBIAN MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
debian_project -- xpdf	In xpdf, the xref table contains an infinite loop which allows remote attackers to cause a denial of service (application crash) in xpdf-based PDF viewers.	2019-10-30	4.3	CVE-2010-0207 MISC MISC
debian_project -- xpdf	xpdf allows remote attackers to cause a denial of service (NULL pointer dereference and crash) in the way it processes JBIG2 PDF stream objects.	2019-10-30	4.3	CVE-2010-0206 MISC MISC
debian_project -- zoo	Zoo 2.10 has Directory traversal	2019-10-28	5	CVE-2005-2349 MISC MISC
devada -- dzone_and_answerhub	An XML External Entity Injection vulnerability exists in Dzone AnswerHub.	2019-10-28	5	CVE-2017-15725 MISC
digium -- asterisk	asterisk allows calls on prohibited networks	2019-10-29	5	CVE-2009-3723 MISC MISC MISC
fabrik -- fabrik	Reflected Cross-Site Scripting (XSS) vulnerability in the fabrik_referrer hidden field in the Fabrikar Fabrik component through v3.8.1 for Joomla! allows remote attackers to inject arbitrary web script via the HTTP Referer header.	2019-10-29	4.3	CVE-2018-10727 MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. 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 processing of Javascript in the HTML2PDF plugin. 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 object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8692.	2019-10-25	6.8	CVE-2019-17139 MISC MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. 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 conversion of DXF files to PDF. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9276.	2019-10-25	6.8	CVE-2019-17145 MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. 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 conversion	2019-10-25	6.8	CVE-2019-17144 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of DWG files to PDF. 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-9274.			
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. 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 processing of script within a Keystroke action of a listbox field. 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-9081.	2019-10-25	6.8	CVE-2019-17142 MISC MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. 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 processing of script within a Calculate action of a text field. 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-9044.	2019-10-25	6.8	CVE-2019-17141 MISC MISC
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.6.0.25114. 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 DWG 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 in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9273.	2019-10-25	4.3	CVE-2019-17143 MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. 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 the OnFocus event. 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-9091.	2019-10-25	6.8	CVE-2019-17140 MISC MISC
foxit -- studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.909. 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 conversion from JPEG to EPS. 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 in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8809.	2019-10-25	4.3	CVE-2019-17138 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnuboard -- gnuboard5	GNUBOARD5 before 5.3.2.0 has XSS that allows remote attackers to inject arbitrary web script or HTML via the "board group extra contents" parameter, aka the adm/boardgroup_form_update.php gr_1~10 parameter.	2019-10-30	4.3	CVE-2018-18678 MISC MISC MISC
gpw -- gpw	gpw generates shorter passwords than required	2019-10-29	5	CVE-2011-4931 MISC MISC MISC MISC
honeywell -- ip-ak2	In IP-AK2 Access Control Panel Version 1.04.07 and prior, the integrated web server of the affected devices could allow remote attackers to obtain web configuration data, which can be accessed without authentication over the network.	2019-10-25	5	CVE-2019-13525 MISC
ibm -- api_connect	IBM API Connect version V5.0.0.0 through 5.0.8.7 could reveal sensitive information to an attacker using a specially crafted HTTP request. IBM X-Force ID: 167883.	2019-10-29	5	CVE-2019-4600 XF CONFIRM
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 162260.	2019-10-25	5	CVE-2019-4399 XF CONFIRM
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 162261.	2019-10-25	4	CVE-2019-4400 XF CONFIRM
ibm -- maximo_asset_management	After installing the IBM Maximo Health- Safety and Environment Manager 7.6.1, a user is granted additional privileges that they are not normally allowed to access. IBM X-Force ID: 165948.	2019-10-29	6.5	CVE-2019-4546 XF CONFIRM
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance could allow unauthenticated attacker to cause a denial of service in the reverse proxy component. IBM X-Force ID: 156159.	2019-10-25	5	CVE-2019-4036 XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 161418.	2019-10-29	5	CVE-2019-4339 XF CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 specifies permissions for a security-critical resource which could lead to the exposure of sensitive information or the modification of that resource by unintended parties. IBM X-Force ID: 160986.	2019-10-29	6.4	CVE-2019-4306 XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 stores sensitive information in cleartext within a resource that might be accessible to another control sphere. IBM X-Force ID: 1610141.	2019-10-29	5	CVE-2019-4314 XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 does not set the secure attribute for cookies in HTTPS sessions, which could cause the user agent to send those cookies in plaintext over an HTTP session. IBM X-Force ID: 161210.	2019-10-29	4.3	CVE-2019-4330 XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 161209.	2019-10-29	4	CVE-2019-4329 XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 161037.	2019-10-29	5	CVE-2019-4311 XF CONFIRM
ikiwiki -- ikiwiki	A cross-site scripting (XSS) vulnerability in ikiwiki before 3.20101112 allows remote attackers to inject arbitrary web script or HTML via a comment.	2019-10-30	4.3	CVE-2010-1673 CONFIRM MISC
ikiwiki -- ikiwiki	Cross Site Scripting (XSS) in ikiwiki before 3.20110122 could allow remote attackers to insert arbitrary JavaScript due to insufficient checking in comments.	2019-10-29	4.3	CVE-2011-0428 CONFIRM MISC
jetbrains -- teamcity	In JetBrains YouTrack before 2019.2.55152, removing tags from the issues list without the corresponding permission was possible.	2019-10-31	5	CVE-2019-18369 CONFIRM
jetbrains -- teamcity	In JetBrains TeamCity before 2019.1.2, access could be gained to the history of builds of a deleted build configuration under some circumstances.	2019-10-31	5	CVE-2019-18363 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
labkey -- labkey_server	An issue was discovered in LabKey Server 19.1.0. It is possible to force a logged-in administrator to execute code through a /reports-viewScriptReport.view CSRF vulnerability.	2019-10-29	6.8	CVE-2019-9926 MISC MISC
labkey -- labkey_server	An issue was discovered in LabKey Server 19.1.0. Sending an SVG containing an XXE payload to the endpoint visualization-exportImage.view or visualization-exportPDF.view allows local files to be read.	2019-10-29	5	CVE-2019-9757 MISC MISC
libpod -- libpod	An issue was discovered in Podman in libpod before 1.6.0. It resolves a symlink in the host context during a copy operation from the container to the host, because an undesired glob operation occurs. An attacker could create a container image containing particular symlinks that, when copied by a victim user to the host filesystem, may overwrite existing files with others from the host.	2019-10-28	5.8	CVE-2019-18466 MISC MISC MISC MISC
mcafee -- mcafee_total_protection	A File Masquerade vulnerability in McAfee Total Protection (MTP) version 16.0.R21 and earlier in Windows client allowed an attacker to read the plaintext list of AV-Scan exclusion files from the Windows registry, and to possibly replace excluded files with potential malware without being detected.	2019-10-28	4.6	CVE-2019-3636 CONFIRM
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension through 1.34 for MediaWiki. Previously hidden (restricted) AbuseFilter filters were viewable (or their differences were viewable) to unprivileged users, thus disclosing potentially sensitive information.	2019-10-29	5	CVE-2019-18612 MISC MISC
mediawiki -- mediawiki	A cross-site scripting (XSS) vulnerability in MediaWiki before 1.19.5 and 1.20.x before 1.20.4 and allows remote attackers to inject arbitrary web script or HTML via Lua function names.	2019-10-31	4.3	CVE-2013-1951 MISC MISC MISC MISC MISC MISC MISC CONFIRM MISC
mediawiki -- mediawiki	An issue was discovered in the CheckUser extension through 1.34 for MediaWiki. Certain sensitive information within oversighted edit summaries made available via the MediaWiki API was potentially visible to users with various levels of access to this extension. Said users should not have been able to view these oversighted edit summaries via the MediaWiki API.	2019-10-29	4	CVE-2019-18611 MISC MISC
mediawiki -- mediawiki	mediawiki allows deleted text to be exposed	2019-10-29	5	CVE-2012-0046 MISC MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mikrotik -- routeros	RouterOS versions 6.45.6 Stable, 6.44.5 Long-term, and below are vulnerable to a DNS unrelated data attack. The router adds all A records to its DNS cache even when the records are unrelated to the domain that was queried. Therefore, a remote attacker controlled DNS server can poison the router's DNS cache via malicious responses with additional and untrue records.	2019-10-29	5	CVE-2019-3979 MISC
mikrotik -- routeros	RouterOS 6.45.6 Stable, RouterOS 6.44.5 Long-term, and below are vulnerable to an arbitrary directory creation vulnerability via the upgrade package's name field. If an authenticated user installs a malicious package then a directory could be created and the developer shell could be enabled.	2019-10-29	6.5	CVE-2019-3976 MISC
mikrotik -- routeros	RouterOS versions 6.45.6 Stable, 6.44.5 Long-term, and below allow remote unauthenticated attackers to trigger DNS queries via port 8291. The queries are sent from the router to a server of the attacker's choice. The DNS responses are cached by the router, potentially resulting in cache poisoning	2019-10-29	5	CVE-2019-3978 MISC MISC
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 have a default set of 10 privileged accounts with hardcoded credentials. They are accessible if the customer has not configured 10 actual user accounts.	2019-10-25	5	CVE-2016-2358 MISC MISC MISC
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 have a default root password in /etc/shadow that is the same across different customers' installations.	2019-10-25	5	CVE-2016-2360 MISC MISC MISC
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 have a hardcoded SSL private key under the /etc/config directory.	2019-10-25	5	CVE-2016-2357 MISC MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. A world-readable /usr/smartrtu/init/settings.xml configuration file on the file system allows an attacker to read sensitive configuration settings such as usernames, passwords, and other sensitive RTU data due to insecure permission assignment.	2019-10-28	4	CVE-2019-14925 MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Stored cleartext passwords could allow an unauthenticated attacker to obtain configured username and password combinations on the RTU due to the weak credentials management on the RTU. An unauthenticated user can obtain the exposed password credentials to gain access to the following services: DDNS service, Mobile Network Provider, and OpenVPN service.	2019-10-28	5	CVE-2019-14929 MISC MISC
mitsubishi_electric_and_inea --	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. An unauthenticated remote	2019-10-28	5	CVE-2019-14927

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
me-rtu_devices	configuration download vulnerability allows an attacker to download the smartRTU's configuration file (which contains data such as usernames, passwords, and other sensitive RTU data).			MISC MISC
netapp -- clustered_data_ontap	Clustered Data ONTAP versions 9.2 through 9.6 are susceptible to a vulnerability which allows an attacker to use l2ping to cause a Denial of Service (DoS).	2019-10-25	5	CVE-2019-5508 MISC
openafs_foundation -- openafs	OpenAFS before 1.6.24 and 1.8.x before 1.8.5 is prone to an information disclosure vulnerability because uninitialized scalars are sent over the network to a peer.	2019-10-29	5	CVE-2019-18602 MISC
openafs_foundation -- openafs	OpenAFS before 1.6.24 and 1.8.x before 1.8.5 is prone to information leakage upon certain error conditions because uninitialized RPC output variables are sent over the network to a peer.	2019-10-29	4.3	CVE-2019-18603 MISC
openafs_foundation -- openafs	OpenAFS before 1.6.24 and 1.8.x before 1.8.5 is prone to denial of service from unserialized data access because remote attackers can make a series of VOTE_Debug RPC calls to crash a database server within the SVOTE_Debug RPC handler.	2019-10-29	5	CVE-2019-18601 MISC
pimcore -- pimcore	Pimcore 6.2.3 has XSS in the translations grid because bundles/AdminBundle/Resources/public/js/pimcore/settings/translations.js mishandles certain HTML elements.	2019-10-31	4.3	CVE-2019-18656 MISC
pixelpost -- pixelpost	pixelpost 1.7.1 has XSS	2019-10-28	4.3	CVE-2009-4900 MISC DEBIAN MISC
python_keyring_lib -- python_keyring_lib	Python keyring lib before 0.10 created keyring files with world-readable permissions.	2019-10-28	5	CVE-2012-5577 MISC CONFIRM MISC MISC MISC
rittal -- rittal_chiller_sk_3232_series	Rittal Chiller SK 3232-Series web interface as built upon Carel pCOWeb firmware A1.5.3 ? B1.2.4. The authentication mechanism on affected systems does not provide a sufficient level of protection against unauthorized configuration changes. Primary operations, namely turning the cooling unit on and off and setting the temperature set point, can be modified without authentication.	2019-10-25	5	CVE-2019-13549 FULLDISC MISC
schneider_electric -- multiple_modic	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the PLC when	2019-10-29	4	CVE-2019-6841 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
on_controllers	upgrading the firmware with no firmware image inside the package using FTP protocol.			
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the PLC when upgrading the firmware with a missing web server image inside the package using FTP protocol.	2019-10-29	4	CVE-2019-6842 CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the PLC when upgrading the controller with an empty firmware package using FTP protocol.	2019-10-29	4	CVE-2019-6843 CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service atack on the PLC when upgrading the controller with a firmware package containing an invalid web server image using FTP protocol.	2019-10-29	4	CVE-2019-6844 CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the FTP service when upgrading the firmware with a version incompatible with the application in the controller using FTP protocol.	2019-10-29	4	CVE-2019-6847 CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-200: Information Exposure vulnerability exists in Modicon M580, Modicon BMENOC 0311, and Modicon BMENOC 0321, which could cause the disclosure of sensitive information when using specific Modbus services provided by the REST API of the controller/communication module.	2019-10-29	5	CVE-2019-6849 CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon BMENOC 0311, and Modicon BMENOC 0321, which could cause a Denial of Service attack on the PLC when sending specific data on the REST API of the controller/communication module.	2019-10-29	5	CVE-2019-6848 CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-200: Information Exposure vulnerability exists in Modicon M580, Modicon BMENOC 0311, and Modicon BMENOC 0321, which could cause the disclosure of sensitive information when reading specific registers with the REST API of the controller/communication module.	2019-10-29	5	CVE-2019-6850 CONFIRM
terramaster -- fs-210_devices	An issue was discovered on TerraMaster FS-210 4.0.19 devices. Normal users can use 1.user.php for privilege elevation.	2019-10-28	6.5	CVE-2019-18195 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tightvnc_software -- tightvnc	TightVNC code version 1.3.10 contains null pointer dereference in HandleZlibBPP function, which results Denial of System (DoS). This attack appear to be exploitable via network connectivity.	2019-10-29	5	CVE-2019-15680 MLIST
tiki_wiki -- cms_groupware	Tiki Wiki CMS Groupware 5.2 has XSS	2019-10-28	4.3	CVE-2010-4240 MISC MISC MISC MISC
tiki_wiki -- cms_groupware	Tiki Wiki CMS Groupware 5.2 has CSRF	2019-10-28	6.8	CVE-2010-4241 MISC MISC MISC MISC
total_defense -- anti-virus	The malware scan function in Total Defense Anti-virus 11.5.2.28 is vulnerable to a TOCTOU bug; consequently, symbolic link attacks allow privileged files to be deleted.	2019-10-31	5.8	CVE-2019-18644 MISC
transmission -- transmission	Transmission before 1.92 allows attackers to prevent download of a file by corrupted data during the endgame.	2019-10-30	5	CVE-2010-0749 MISC CONFIRM MISC CONFIRM MLIST
trend_micro -- apex_one	Trend Micro Apex One could be exploited by an attacker utilizing a command injection vulnerability to extract files from an arbitrary zip file to a specific folder on the Apex One server, which could potentially lead to remote code execution (RCE). The remote process execution is bound to the IUSR account, which has restricted permission and is unable to make major system changes. An attempted attack requires user authentication.	2019-10-28	5	CVE-2019-18188 N/A
trend_micro -- office_scan	Trend Micro OfficeScan versions 11.0 and XG (12.0) could be exploited by an attacker utilizing a directory traversal vulnerability to extract files from an arbitrary zip file to a specific folder on the OfficeScan server, which could potentially lead to remote code execution (RCE). The remote process execution is bound to a web service account, which depending on the web platform used may have restricted permissions. An attempted attack requires user authentication.	2019-10-28	5	CVE-2019-18187 N/A
youphptube -- youphptube	An exploitable SQL injection vulnerability exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configurations, access the underlying operating system.	2019-10-25	6.5	CVE-2019-5120 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
youphptube -- youphptube	SQL injection vulnerabilities exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with Parameter name in /objects/pluginSwitch.json.php.	2019-10-25	6.5	CVE-2019-5122 MISC
youphptube -- youphptube	SQL injection vulnerabilities exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with Parameter uuid in /objects/pluginSwitch.json.php	2019-10-25	6.5	CVE-2019-5121 MISC
youphptube -- youphptube	An exploitable SQL injection vulnerability exist in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configurations, access the underlying operating system.	2019-10-25	6.5	CVE-2019-5119 MISC
youphptube -- youphptube	Exploitable SQL injection vulnerabilities exists in the authenticated portion of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configuration, access the underlying operating system.	2019-10-25	6.5	CVE-2019-5117 MISC
youphptube -- youphptube	An exploitable SQL injection vulnerability exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause a SQL injection. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configuration, access the underlying operating system.	2019-10-25	6.5	CVE-2019-5116 MISC
youphptube -- youphptube	An exploitable SQL injection vulnerability exists in the authenticated portion of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and,in certain configuration, access the underlying operating system.	2019-10-25	6.5	CVE-2019-5114 MISC
youphptube -- youphptube	Specially crafted web requests can cause SQL injections in YouPHPTube 7.6. An attacker can send a web request with Parameter dir in /objects/pluginSwitch.json.php.	2019-10-25	6.5	CVE-2019-5123 MISC
zucchetti -- infobusiness	Multiple Reflected Cross-site Scripting (XSS) vulnerabilities exist in Zucchetti InfoBusiness before and including 4.4.1. The browsing component did not properly sanitize user input (encoded in base64). This also applies to the search functionality for the searchKey parameter.	2019-10-30	4.3	CVE-2019-18205 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zucchetti -- infobusiness	Zucchetti InfoBusiness before and including 4.4.1 allows any authenticated user to upload .php files in order to achieve code execution.	2019-10-30	6.5	CVE-2019-18204 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- airflow	A malicious admin user could edit the state of objects in the Airflow metadata database to execute arbitrary javascript on certain page views. This also presented a Local File Disclosure vulnerability to any file readable by the webserver process.	2019-10-30	3.5	CVE-2019-12417 MLIST
d-link -- dir-865l_devices	D-Link DIR-865L has Information Disclosure.	2019-10-25	2.9	CVE-2013-4856 MISC MISC MISC
debian_project -- mailscanner	mailscanner can allow local users to prevent virus signatures from being updated	2019-10-28	2.1	CVE-2010-3293 MISC DEBIAN MISC MISC
debian_project -- paxtext	paxtest handles temporary files insecurely	2019-10-29	2.1	CVE-2010-3373 MISC MISC MISC
gmer -- gmer	A stack based buffer overflow vulnerability exists in the method receiving data from SysTreeView32 control of the GMER 2.1.19357 application. A specially created long path can lead to a buffer overflow on the stack resulting in code execution. An attacker needs to create path longer than 99 characters to trigger this vulnerability.	2019-10-29	2.1	CVE-2016-4289 MISC
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 could allow a local user to obtain sensitive information from temporary script files. IBM X-Force ID: 162333.	2019-10-25	2.1	CVE-2019-4395 XF CONFIRM
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 is vulnerable to HTTP response splitting attacks, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to inject arbitrary HTTP headers and cause the server to return a split response, once the URL is clicked. This would allow the attacker to perform further attacks, such as Web cache poisoning or cross-site scripting, and possibly obtain sensitive information. IBM X-Force ID: 162236.	2019-10-25	3.5	CVE-2019-4396 XF CONFIRM
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 is vulnerable to HTTP Response Splitting caused by improper caching of content. This would allow the attacker to perform further attacks, such as Web	2019-10-25	3.5	CVE-2019-4461 XF CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Cache poisoning, cross-site scripting and possibly obtain sensitive information. IBM X-Force ID: 163682.			
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 contain APIs that could be used by a local user to send email. IBM X-Force ID: 162232.	2019-10-25	2.1	CVE-2019-4394 XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 160987.	2019-10-29	2.1	CVE-2019-4307 XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 uses hard coded credentials which could allow a local user to obtain highly sensitive information. IBM X-Force ID: 161035.	2019-10-29	2.1	CVE-2019-4309 XF CONFIRM
labkey -- labkey_server	An issue was discovered in LabKey Server 19.1.0. The display name of a user is vulnerable to stored XSS that can execute on administrators from security/permissions.view, security/addUsers.view, or wiki/Administration/page.view in the admin panel, leading to privilege escalation.	2019-10-29	3.5	CVE-2019-9758 MISC MISC
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in the configuration report page (adm_config_report.php) in MantisBT 1.2.0rc1 before 1.2.14 allows remote authenticated users to inject arbitrary web script or HTML via a complex value.	2019-10-31	3.5	CVE-2013-1934 MISC MISC MISC CONFIRM MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. A number of stored cross-site script (XSS) vulnerabilities allow an attacker to inject malicious code directly into the application. An example input variable vulnerable to stored XSS is SerialInitialModemString in the index.php page.	2019-10-28	3.5	CVE-2019-14928 MISC MISC
postgresql -- postgresql	Postgresql, versions 11.x before 11.5, is vulnerable to a memory disclosure in cross-type comparison for hashed subplan.	2019-10-29	3.5	CVE-2019-10209 CONFIRM CONFIRM
postgresql -- postgresql_windows_installer	Postgresql Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable via superuser writing password to unprotected temporary file.	2019-10-29	1.9	CVE-2019-10210 CONFIRM CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
total_defense -- antivirus	The quarantine restoration function in Total Defense Anti-virus 11.5.2.28 is vulnerable to symbolic link attacks, allowing files to be written to privileged directories.	2019-10-31	2.1	CVE-2019-18645 MISC