Vulnerability Summary for the Week of May 10, 2021

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by Ug-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of Ug-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
artica -- pandora_fms	A SQL injection vulnerability in the pandora_console component of Artica Pandora FMS 742 allows an unauthenticated attacker to upgrade his unprivileged session via the /include/chart_generator.php session_id parameter, leading to a login bypass.	2021-05-07	7.5	CVE-2021-32099 MISC MISC MISC
artica -- pandora_fms	Artica Pandora FMS 742 allows unauthenticated attackers to perform Phar deserialization.	2021-05-07	7.5	CVE-2021-32098 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.3, argument injection leading to remote code execution was possible.	2021-05-11	7.5	CVE-2021-31909 MISC MISC
microsoft -- windows_10	HTTP Protocol Stack Remote Code Execution Vulnerability	2021-05-11	7.5	CVE-2021-31166 N/A
qualcomm -- apq8009_firmware	Memory corruption while processing crafted SDES packets due to improper length check in sdes packets recieved in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-05-07	10	CVE-2020-11279 CONFIRM
qualcomm -- apq8009_firmware	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	2021-05-07	10	CVE-2021-1910 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables			
qualcomm -- apq8009_firmware	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-05-07	7.2	CVE-2021-1905 CONFIRM
qualcomm -- apq8009_firmware	Out of bound write can occur in TZ command handler due to lack of validation of command ID in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-05-07	7.2	CVE-2020-11289 CONFIRM
qualcomm -- apq8009_firmware	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-05-07	7.2	CVE-2021-1927 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- apq8009_firmware	Buffer over-read while unpacking the RTCP packet we may read extra byte if wrong length is provided in RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-05-07	9.4	CVE-2020-11285 CONFIRM
qualcomm -- apq8009w_firmware	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	2021-05-07	7.2	CVE-2021-1895 CONFIRM
qualcomm -- apq8096au_firmware	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	2021-05-07	7.2	CVE-2021-1915 CONFIRM
qualcomm -- aqt1000_firmware	Denial of service in MODEM due to assert to the invalid configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	2021-05-07	7.8	CVE-2020-11274 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- aqt1000_firmware	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	2021-05-07	7.8	CVE-2021-1925 CONFIRM
qualcomm -- aqt1000_firmware	Locked memory can be unlocked and modified by non secure boot loader through improper system call sequence making the memory region untrusted source of input for secure boot loader in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-05-07	7.2	CVE-2020-11284 CONFIRM
qualcomm -- aqt1000_firmware	Out of bound write can occur in playready while processing command due to lack of input validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	2021-05-07	7.2	CVE-2020-11288 CONFIRM
qualcomm -- csrb31024_firmware	Histogram type KPI was teardown with the assumption of the existence of histogram binning info and will lead to null pointer access when histogram binning info is missing due to lack of null check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile	2021-05-07	7.8	CVE-2020-11273 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
remotemouse -- emote_remote_mouse	An issue was discovered in Emote Remote Mouse through 4.0.0.0. Remote unauthenticated users can execute arbitrary code via crafted UDP packets with no prior authorization or authentication.	2021-05-07	7.5	CVE-2021-27573 MISC MISC
stacklift -- localstack	The dashboard component of StackLift LocalStack 0.12.6 allows attackers to inject arbitrary shell commands via the functionName parameter.	2021-05-07	10	CVE-2021-32090 MISC MISC
tenda -- ac11_firmware	An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setportList allows attackers to execute arbitrary code on the system via a crafted post request.	2021-05-07	10	CVE-2021-31758 MISC
tenda -- ac11_firmware	An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setVLAN allows attackers to execute arbitrary code on the system via a crafted post request.	2021-05-07	10	CVE-2021-31757 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenda -- ac11_firmware	An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setwanType allows attackers to execute arbitrary code on the system via a crafted post request. This occurs when input vector controlled by malicious attack get copied to the stack variable.	2021-05-07	10	CVE-2021-31756 MISC
tenda -- ac11_firmware	An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setmac allows attackers to execute arbitrary code on the system via a crafted post request.	2021-05-07	10	CVE-2021-31755 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
5none -- nonecms	NoneCMS v1.3 has a CSRF vulnerability in public/index.php/admin/nav/add.html, as	2021-05-10	4.3	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	demonstrated by adding a navigation column which can be injected with arbitrary web script or HTML via the name parameter to launch a stored XSS attack.			23376 MISC
5none -- nonecms	Cross-site scripting (XSS) vulnerability in static/admin/js/kindeditor/plugins/multiimage/images/swfupload.swf in noneCms v1.3.0 allows remote attackers to inject arbitrary web script or HTML via the movieName parameter.	2021-05-10	4.3	CVE-2020-23371 MISC
artica -- pandora_fms	A remote file inclusion vulnerability exists in Artica Pandora FMS 742, exploitable by the lowest privileged user.	2021-05-07	4	CVE-2021-32100 MISC MISC MISC
atlassian -- confluence	Affected versions of Confluence Server before 7.11.0 allow attackers to identify internal hosts and ports via a blind server-side request forgery vulnerability in Team Calendars parameters.	2021-05-07	4	CVE-2020-29445 N/A

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
craftcms -- craft_cms	Craft CMS before 3.6.13 has an XSS vulnerability.	2021-05-07	4.3	CVE-2021-32470 MISC MISC
eng -- knowage	Knowage Suite 7.3 is vulnerable to unauthenticated reflected cross-site scripting (XSS). An attacker can inject arbitrary web script in '/servlet/AdapterHTTP' via the 'targetService' parameter.	2021-05-12	4.3	CVE-2021-30213 MISC
eventlet -- eventlet	Eventlet is a concurrent networking library for Python. A websocket peer may exhaust memory on Eventlet side by sending very large websocket frames. Malicious peer may exhaust memory on Eventlet side by sending highly compressed data frame. A patch in version 0.31.0 restricts websocket frame to reasonable limits. As a workaround, restricting memory usage via OS limits would help against overall machine exhaustion, but there is no workaround to protect Eventlet process.	2021-05-07	5	CVE-2021-21419 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. 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-13273.	2021-05-07	4.3	CVE-2021-31448 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the	2021-05-07	6.8	CVE-2021-31441 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13101.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 Annotation objects. 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-13089.	2021-05-07	6.8	CVE-2021-31451 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 validating the	2021-05-07	6.8	CVE-2021-31449 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	existence of an object prior to performing further free operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13280.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13239.	2021-05-07	6.8	CVE-2021-31442 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a	2021-05-07	4.3	CVE-2021-31443 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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-13240.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. 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	2021-05-07	4.3	CVE-2021-31444 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	context of the current process. Was ZDI-CAN-13241.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. 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-13244.	2021-05-07	4.3	CVE-2021-31445 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The	2021-05-07	4.3	CVE-2021-31446 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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-13245.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. 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-13269.	2021-05-07	4.3	CVE-2021-31447 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 XFA forms. 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-13084.	2021-05-07	6.8	CVE-2021-31450 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 XFA forms. 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-13100.	2021-05-07	6.8	CVE-2021-31455 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 Decimal element. A crafted leadDigits value in a Decimal element can trigger an overflow of a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute arbitrary code in the context of the current process. Was ZDI-CAN-13095.	2021-05-07	6.8	CVE-2021-31454 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 XFA Forms. 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	2021-05-07	6.8	CVE-2021-31453 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	code in the context of the current process. Was ZDI-CAN-13092.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 XFA forms. 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 data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13091.	2021-05-07	6.8	CVE-2021-31452 MISC MISC
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 Annotation objects. The issue results from the lack of validating the existence of an	2021-05-07	6.8	CVE-2021-31456 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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-13102.			
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 the handling of app.media objects. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process Was ZDI-CAN-13333.	2021-05-07	6.8	CVE-2021-31461 MISC MISC
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 XFA templates. The issue results	2021-05-07	6.8	CVE-2021-31460 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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-13096.			
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 XFA Forms. 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-13162.	2021-05-07	6.8	CVE-2021-31459 MISC MISC
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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	2021-05-07	6.8	CVE-2021-31458 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	handling of Annotation objects. 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-13150.			
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. 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 Annotation objects. 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-13147.	2021-05-07	6.8	CVE-2021-31457 MISC MISC
hashicorp -- vault-action	HashiCorp vault-action (aka Vault GitHub Action) before 2.2.0 allows attackers to obtain sensitive information from log files because a multi-line secret was not correctly registered with GitHub Actions for log masking.	2021-05-07	5	CVE-2021-32074 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.5.0.0 and 1.5.0.1 could allow a user to obtain sensitive information or perform actions they should not have access to due to incorrect authorization mechanisms. IBM X-Force ID: 198919.	2021-05-10	6.4	CVE-2021-20538 XF CONFIRM
ibm -- cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.5.0.0 and 1.5.0.1 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: 199281.	2021-05-10	4.3	CVE-2021-20577 CONFIRM XF
ibm -- openpages_grc_platform	IBM OpenPages GRC Platform 8.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 182907.	2021-05-11	4	CVE-2020-4536 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11.0 could allow an attacker on the network to obtain sensitive information or cause a denial of service through username enumeration. IBM X-Force ID: 190992.	2021-05-07	6.4	CVE-2020-4901 CONFIRM XF
jenkins -- credentials	Jenkins Credentials Plugin 2.3.18 and earlier does not escape user-controlled information on a view it provides, resulting in a reflected cross-site scripting (XSS) vulnerability.	2021-05-11	4.3	CVE-2021-21648 CONFIRM
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA before 2021.1, DoS was possible because of unbounded resource allocation.	2021-05-11	5	CVE-2021-30504 MISC MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.2, audit logs were not sufficient when an administrator uploaded a file.	2021-05-11	4	CVE-2021-31906 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.2, permission checks for changing TeamCity plugins were implemented improperly.	2021-05-11	5	CVE-2021-31907 MISC MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.3, reflected XSS was possible on several pages.	2021-05-11	4.3	CVE-2021-31911 MISC MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.2, XSS was potentially possible on the test history page.	2021-05-11	4.3	CVE-2021-31904 MISC MISC
jetbrains -- youtrack	In JetBrains YouTrack before 2020.6.8801, information disclosure in an issue preview was possible.	2021-05-11	5	CVE-2021-31905 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	net/bluetooth/hci_request.c in the Linux kernel through 5.12.2 has a race condition for removal of the HCI controller.	2021-05-10	4.4	CVE-2021-32399 MISC MISC MLIST
livinglogic -- xist4c	LivingLogic XIST4C before 0.107.8 allows XSS via feedback.htm or feedback.wihtm.	2021-05-07	4.3	CVE-2021-26122 MISC MISC
livinglogic -- xist4c	LivingLogic XIST4C before 0.107.8 allows XSS via login.htm, login.wihtm, or login-form.htm.	2021-05-07	4.3	CVE-2021-26123 MISC MISC
microsoft -- windows_10	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31165, CVE-2021-31167, CVE-2021-31169, CVE-2021-31208.	2021-05-11	4.6	CVE-2021-31168 N/A MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Hyper-V Remote Code Execution Vulnerability	2021-05-11	6.5	CVE-2021-28476 N/A
microsoft -- windows_10	Windows Graphics Component Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31188.	2021-05-11	4.6	CVE-2021-31170 N/A MISC
microsoft -- windows_10	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31165, CVE-2021-31167, CVE-2021-31168, CVE-2021-31208.	2021-05-11	4.6	CVE-2021-31169 N/A MISC
microsoft -- windows_10	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31167, CVE-2021-31168, CVE-2021-31169, CVE-2021-31208.	2021-05-11	4.6	CVE-2021-31165 N/A MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31165, CVE-2021-31168, CVE-2021-31169, CVE-2021-31208.	2021-05-11	4.6	CVE-2021-31167 N/A MISC
nim-lang -- nim	Nim is a statically typed compiled systems programming language. In Nim standard library before 1.4.2, httpClient SSL/TLS certificate verification was disabled by default. Users can upgrade to version 1.4.2 to receive a patch or, as a workaround, set "verifyMode = CVerifyPeer" as documented.	2021-05-07	5	CVE-2021-29495 CONFIRM
nsa -- emissary	A Cross-site scripting (XSS) vulnerability in the DocumentAction component of U.S. National Security Agency (NSA) Emissary 5.9.0 allows remote attackers to inject arbitrary web script or HTML via the uuid parameter.	2021-05-07	4.3	CVE-2021-32092 MISC MISC
nsa -- emissary	The ConfigFileAction component of U.S. National Security Agency (NSA) Emissary 5.9.0 allows an authenticated user to read arbitrary files via the ConfigName parameter.	2021-05-07	4	CVE-2021-32093

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
nsa -- emissary	U.S. National Security Agency (NSA) Emissary 5.9.0 allows an authenticated user to upload arbitrary files.	2021-05-07	6.5	CVE-2021-32094 MISC MISC
nsa -- emissary	U.S. National Security Agency (NSA) Emissary 5.9.0 allows an authenticated user to delete arbitrary files.	2021-05-07	5.5	CVE-2021-32095 MISC MISC
open-emr -- openemr	The Patient Portal of OpenEMR 5.0.2.1 is affected by a incorrect access control system in portal/patient/_machine_config.php. To exploit the vulnerability, an unauthenticated attacker can register an account, bypassing the permission check of this portal's API. Then, the attacker can then manipulate and read data of every registered patient.	2021-05-07	6.4	CVE-2021-32101 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
open-emr -- openemr	A SQL injection vulnerability exists (with user privileges) in interface/forms/eye_mag/save.php in OpenEMR 5.0.2.1.	2021-05-07	6.5	CVE-2021-32104 MISC MISC MISC MISC MISC
open-emr -- openemr	A SQL injection vulnerability exists (with user privileges) in library/custom_template/ajax_code.php in OpenEMR 5.0.2.1.	2021-05-07	6.5	CVE-2021-32102 MISC MISC MISC MISC MISC
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'listImmoLabels.jsp' page of OpenClinic GA 5.173.3 application. The immoCode parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-05-11	6.5	CVE-2020-27244 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openclinic_ga_project -- openclinic_ga	A number of exploitable SQL injection vulnerabilities exists in ‘patientslist.do’ page of OpenClinic GA 5.173.3 application. The findSector parameter in ‘‘patientslist.do’ page is vulnerable to authenticated SQL injection An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-05-10	6.5	CVE-2020-27230 MISC
openclinic_ga_project -- openclinic_ga	A number of exploitable SQL injection vulnerabilities exists in ‘patientslist.do’ page of OpenClinic GA 5.173.3 application. The findDistrict parameter in ‘‘patientslist.do’ page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-05-10	6.5	CVE-2020-27231 MISC
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in ‘manageServiceStocks.jsp’ page of OpenClinic GA 5.173.3. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-05-10	6.5	CVE-2020-27232 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'listImmoLabels.jsp' page of OpenClinic GA 5.173.3 application. The immoLocation parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-05-11	6.5	CVE-2020-27242 MISC
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'listImmoLabels.jsp' page of OpenClinic GA 5.173.3 application. The immoService parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-05-11	6.5	CVE-2020-27243 MISC
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'listImmoLabels.jsp' page of OpenClinic GA 5.173.3 application. The immoComment parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-05-11	6.5	CVE-2020-27246 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'listImmoLabels.jsp' page of OpenClinic GA 5.173.3 application. The immoBuyer parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-05-11	6.5	CVE-2020-27245 MISC
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'quickFile.jsp' page of OpenClinic GA 5.173.3. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-05-10	6.5	CVE-2020-27226 MISC
openclinic_ga_project -- openclinic_ga	A number of exploitable SQL injection vulnerabilities exists in 'patientslist.do' page of OpenClinic GA 5.173.3 application. The findPersonID parameter in ''patientslist.do' page is vulnerable to authenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-05-10	6.5	CVE-2020-27229 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
paxtechnology -- paxstore	Pax Technology PAXSTORE v7.0.8_20200511171508 and lower is affected by a token spoofing vulnerability. Each payment terminal has a session token (called X-Terminal-Token) to access the marketplace. This allows the store to identify the terminal and make available the applications distributed by its reseller. By intercepting HTTPS traffic from the application store, it is possible to collect the request responsible for assigning the X-Terminal-Token to the terminal, which makes it possible to craft an X-Terminal-Token pretending to be another device. An attacker can use this behavior to authenticate its own payment terminal in the application store through token impersonation.	2021-05-07	6.4	CVE-2020-36128 MISC MISC MISC
paxtechnology -- paxstore	Pax Technology PAXSTORE v7.0.8_20200511171508 and lower is affected by incorrect access control where password revalidation in sensitive operations can be bypassed remotely by an authenticated attacker through requesting the endpoint directly.	2021-05-07	5.5	CVE-2020-36125 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
paxtechnology -- paxstore	Pax Technology PAXSTORE v7.0.8_20200511171508 and lower is affected by incorrect access control that can lead to remote privilege escalation. PAXSTORE marketplace endpoints allow an authenticated user to read and write data not owned by them, including third-party users, application and payment terminals, where an attacker can impersonate any user which may lead to the unauthorized disclosure, modification, or destruction of information.	2021-05-07	5.5	CVE-2020-36126 MISC MISC MISC
paxtechnology -- paxstore	Pax Technology PAXSTORE v7.0.8_20200511171508 and lower is affected by XML External Entity (XXE) injection. An authenticated attacker can compromise the private keys of a JWT token and reuse them to manipulate the access tokens to access the platform as any desired user (clients and administrators).	2021-05-07	4	CVE-2020-36124 MISC MISC MISC
paxtechnology -- paxstore	Pax Technology PAXSTORE v7.0.8_20200511171508 and lower is affected by an information disclosure vulnerability. Through the PUK signature functionality, an	2021-05-07	4	CVE-2020-36127 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	administrator will not have access to the current p12 certificate and password. When accessing this functionality, the administrator has the option to replace the current certificate and it is not possible to view the certificate password (p12) already deployed on the platform. The replacement p12 certificate returns to users in base64 with its password, which can be accessed by non-administrator users.			MISC MISC
qualcomm -- apq8009	Potential UE reset while decoding a crafted Sib1 or SIB1 that schedules unsupported SIBs and can lead to denial of service in Snapdragon Auto, Snapdragon Mobile	2021-05-07	5	CVE-2020-11268 CONFIRM
qualcomm -- ar8035_firmware	Out of bound write in logger due to prefix size is not validated while prepended to logging string in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-05-07	4.6	CVE-2020-11294 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- fsm10055_firmware	Use after free in camera If the threadmanager is being cleaned up while the worker thread is processing objects in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	2021-05-07	4.6	CVE-2020-11295 CONFIRM
remotemouse -- emote_remote_mouse	An issue was discovered in Emote Remote Mouse through 4.0.0.0. It uses cleartext HTTP to check, and request, updates. Thus, attackers can machine-in-the-middle a victim to download a malicious binary in place of the real update, with no SSL errors or warnings.	2021-05-07	6.8	CVE-2021-27574 MISC MISC
remotemouse -- emote_remote_mouse	An issue was discovered in Emote Remote Mouse through 4.0.0.0. Attackers can retrieve recently used and running applications, their icons, and their file paths. This information is sent in cleartext and is not protected by any authentication logic.	2021-05-07	5	CVE-2021-27571 MISC MISC
remotemouse -- emote_remote_mouse	An issue was discovered in Emote Remote Mouse through 4.0.0.0. Attackers can maximize or minimize the window of a running process by	2021-05-07	5	CVE-2021-27569

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sending the process name in a crafted packet. This information is sent in cleartext and is not protected by any authentication logic.			MISC MISC
remotemouse -- emote_remote_mouse	An issue was discovered in Emote Remote Mouse through 3.015. Attackers can close any running process by sending the process name in a specially crafted packet. This information is sent in cleartext and is not protected by any authentication logic.	2021-05-07	5	CVE-2021-27570 MISC MISC
stacklift -- localstack	A Cross-site scripting (XSS) vulnerability exists in StackLift LocalStack 0.12.6.	2021-05-07	4.3	CVE-2021-32091 MISC MISC
yzmcms -- yzmcms	In YzmCMS 5.6, XSS was discovered in member/member_content/init.html via the SRC attribute of an IFRAME element because of using UEditor 1.4.3.3.	2021-05-10	4.3	CVE-2020-23369 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
5none -- nonecms	Cross-site scripting (XSS) vulnerability in admin/nav/add.html in noneCMS v1.3.0 allows remote authenticated attackers to inject arbitrary web script or HTML via the name parameter.	2021-05-10	3.5	CVE-2020-23373 MISC
5none -- nonecms	Cross-site scripting (XSS) vulnerability in admin/article/add.html in noneCMS v1.3.0 allows remote authenticated attackers to inject arbitrary web script or HTML via the name parameter.	2021-05-10	3.5	CVE-2020-23374 MISC
atlassian -- confluence	Affected versions of Team Calendar in Confluence Server before 7.11.0 allow attackers to inject arbitrary HTML or Javascript via a Cross Site Scripting Vulnerability in admin global setting parameters.	2021-05-07	3.5	CVE-2020-29444 N/A
eng -- knowage	Knowage Suite 7.3 is vulnerable to Stored Cross-Site Scripting (XSS). An attacker can inject arbitrary web script in	2021-05-12	3.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	'/knowage/restful-services/signup/update' via the 'surname' parameter.			30211 MISC
eng -- knowage	Knowage Suite 7.3 is vulnerable to Stored Cross-Site Scripting (XSS). An attacker can inject arbitrary web script in '/knowage/restful-services/documentnotes/saveNote' via the 'nota' parameter.	2021-05-12	3.5	CVE-2021-30212 MISC
eng -- knowage	Knowage Suite 7.3 is vulnerable to Stored Client-Side Template Injection in '/knowage/restful-services/signup/update' via the 'name' parameter.	2021-05-12	3.5	CVE-2021-30214 MISC
ibm -- control_desk	IBM Control Desk 7.6.1.2 and 7.6.1.3 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: 199228.	2021-05-10	3.5	CVE-2021-20559 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- openpages_grc_platform	IBM OpenPages GRC Platform 8.1 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: 182906.	2021-05-11	3.5	CVE-2020-4535 CONFIRM XF
igt\+_project -- igt\+	Special characters of IGT search function in igt+ are not filtered in specific fields, which allow remote authenticated attackers can inject malicious JavaScript and carry out DOM-based XSS (Cross-site scripting) attacks.	2021-05-11	3.5	CVE-2021-32544 CONFIRM
jenkins -- dashboard_view	Jenkins Dashboard View Plugin 2.15 and earlier does not escape URLs referenced in Image Dashboard Portlets, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with View/Configure permission.	2021-05-11	3.5	CVE-2021-21649 CONFIRM
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.2, stored XSS on a tests page was possible.	2021-05-11	3.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				3315 MISC MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.3, stored XSS was possible on several pages.	2021-05-11	3.5	CVE-2021-31908 MISC MISC
juhnetec -- enterprise_resource_planning_point_of_sale_system	Special characters of ERP POS customer profile page are not filtered in users' input, which allow remote authenticated attackers can inject malicious JavaScript and carry out stored XSS (Stored Cross-site scripting) attacks, additionally access and manipulate customer's information.	2021-05-07	3.5	CVE-2021-30170 MISC
juhnetec -- enterprise_resource_planning_point_of_sale_system	Special characters of ERP POS news page are not filtered in users' input, which allow remote authenticated attackers can inject malicious JavaScript and carry out stored XSS (Stored Cross-site scripting) attacks,	2021-05-07	3.5	CVE-2021-30171 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	additionally access and manipulate customer's information.			
junhetec -- omnidirectional_communication_system	Special characters of picture preview page in the Quan-Fang-Wei-Tong-Xun system are not filtered in users' input, which allow remote authenticated attackers can inject malicious JavaScript and carry out Reflected XSS (Cross-site scripting) attacks, additionally access and manipulate customer's information.	2021-05-07	3.5	CVE-2021-30172 MISC
microsoft -- windows_10	Windows CSC Service Information Disclosure Vulnerability	2021-05-11	2.1	CVE-2021-28479 N/A
open-emr -- openemr	A Stored XSS vulnerability in interface/usergroup/usergroup_admin.php in OpenEMR before 5.0.2.1 allows a admin authenticated user to inject arbitrary web script or HTML via the lname parameter.	2021-05-07	3.5	CVE-2021-32103 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- apq8009_firmware	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-05-07	2.1	CVE-2021-1906 CONFIRM
qualcomm -- apq8017_firmware	Out of bound read can happen in Widevine TA while copying data to buffer from user data due to lack of check of buffer length received in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-05-07	3.6	CVE-2020-11293 CONFIRM
qualcomm -- pm6150a	Memory corruption during buffer allocation due to dereferencing session ctx pointer without checking if pointer is valid in Snapdragon Auto, Snapdragon Compute,	2021-05-07	2.1	CVE-2020-11254 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Snapdragon Connectivity, Snapdragon Mobile			
yzmcms -- yzmcms	In YzmCMS 5.6, stored XSS exists via the common/static/plugin/ueditor/1.4.3.3/php/controller.php action parameter, which allows remote attackers to upload a swf file. The swf file can be injected with arbitrary web script or HTML.	2021-05-10	3.5	CVE-2020-23370 MISC