Vulnerability Summary for the Week of April 12, 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
dreamreport -- dream_report	A privilege escalation vulnerability exists in Dream Report 5 R20-2. In the default configuration, the Syncfusion Dashboard Service service binary can be replaced by attackers to escalate privileges to NT SYSTEM. An attacker can provide a malicious file to trigger this vulnerability.	2021-04-09	7.2	CVE-2020-13532 MISC
fluidsynth -- fluidsynth	FluidSynth 2.1.7 contains a use after free vulnerability in sfloader/fluid_sffile.c that can result in arbitrary code execution or a denial of service (DoS) if a malicious soundfont2 file is loaded into a fluidsynth library.	2021-04-13	7.5	CVE-2021-28421 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In rw_mfc_handle_read_op of rw_mfc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution via a malicious NFC packet with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-178725766	2021-04-13	10	CVE-2021-0430 MISC
indionetworks -- unibox_u50_firmware	Unibox SMB 2.4 and UniBox Enterprise Series 2.4 and UniBox Campus Series 2.4 contain a cross-site request forgery (CSRF) vulnerability in /tools/network-trace, /list_users, /list_byod?usertype=raduser, /dhcp_leases, /go?rid=202 in which a specially crafted HTTP request may reconfigure the device.	2021-04-09	9.3	CVE-2020-21884 MISC MISC MISC
indionetworks -- unibox_u50_firmware	Unibox U-50 2.4 and UniBox Enterprise Series 2.4 and UniBox Campus Series 2.4 contain a OS command injection vulnerability in /tools/ping, which can leads to complete device takeover.	2021-04-09	9	CVE-2020-21883 MISC MISC MISC
microsoft -- exchange_server	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28481, CVE-2021-28482, CVE-2021-28483.	2021-04-13	10	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				28480 MISC
microsoft -- exchange_server	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28480, CVE-2021-28482, CVE-2021-28483.	2021-04-13	10	CVE-2021-28481 MISC
microsoft -- exchange_server	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28480, CVE-2021-28481, CVE-2021-28483.	2021-04-13	9	CVE-2021-28482 MISC
microsoft -- exchange_server	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28480, CVE-2021-28481, CVE-2021-28482.	2021-04-13	7.7	CVE-2021-28483 MISC
microsoft -- windows_10	Azure AD Web Sign-in Security Feature Bypass Vulnerability	2021-04-13	7.5	CVE-2021-27092 MISC
microsoft -- windows_10	Windows Hyper-V Denial of Service Vulnerability	2021-04-13	7.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				26416 MISC
online_book_store_project -- online_book_store	SQL injection in admin.php in Online Book Store 1.0 allows remote attackers to execute arbitrary SQL commands and bypass authentication.	2021-04-09	7.5	CVE-2020-23763 MISC MISC
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'getAssets.jsp' page of OpenClinic GA 5.173.3 in the compnomenclature parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-04-13	7.5	CVE-2020-27236 MISC
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'getAssets.jsp' page of OpenClinic GA 5.173.3 in the description parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-04-13	7.5	CVE-2020-27235 MISC
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'getAssets.jsp' page of OpenClinic GA 5.173.3 in the serviceUID parameter. An attacker can make an	2021-04-13	7.5	CVE-2020-27234 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated HTTP request to trigger this vulnerability.			
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'getAssets.jsp' page of OpenClinic GA 5.173.3 in the supplierUID parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-04-13	7.5	CVE-2020-27233 MISC
rust-lang -- rust	In the standard library in Rust before 1.53.0, a double free can occur in the Vec::from_iter function if freeing the element panics.	2021-04-14	7.5	CVE-2021-31162 MISC MISC
sonicwall -- email_security	A vulnerability in the SonicWall Email Security version 10.0.9.x allows an attacker to create an administrative account by sending a crafted HTTP request to the remote host.	2021-04-09	7.5	CVE-2021-20021 CONFIRM
sonicwall -- global_management_system	A command execution vulnerability in SonicWall GMS 9.3 allows a remote unauthenticated attacker to locally escalate privilege to root.	2021-04-10	10	CVE-2021-20020 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One, Trend Micro Apex One as a Service and OfficeScan XG SP1 on a sensitive file could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2021-04-13	7.2	CVE-2021-25250 N/A N/A N/A
trendmicro -- apex_one	An improper access control vulnerability in Trend Micro Apex One, Trend Micro Apex One as a Service and OfficeScan XG SP1 on a resource used by the service could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2021-04-13	7.2	CVE-2021-25253 N/A N/A N/A
trendmicro -- apex_one	An incorrect permission assignment vulnerability in Trend Micro Apex One, Apex One as a Service and OfficeScan XG SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2021-04-13	7.2	CVE-2021-28645 N/A N/A N/A

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
windriver -- vxworks	An issue was discovered in Wind River VxWorks before 6.5. There is a possible heap overflow in dhcp client.	2021-04-13	7.5	CVE-2021-29998 MISC
windriver -- vxworks	An issue was discovered in Wind River VxWorks through 6.8. There is a possible stack overflow in dhcp server.	2021-04-13	7.5	CVE-2021-29999 MISC
zerof -- expert	The ZEROF Expert pro/2.0 application for mobile devices allows SQL Injection via the Authorization header to the /v2/devices/add endpoint.	2021-04-13	7.5	CVE-2021-30176 MISC MISC
zerof -- web_server	ZEROF Web Server 1.0 (April 2021) allows SQL Injection via the /HandleEvent endpoint for the login page.	2021-04-13	7.5	CVE-2021-30175 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accessally -- accessally	In the AccessAlly WordPress plugin before 3.5.7, the file "resource/frontend/product/product-shortcode.php" responsible for the [accessally_order_form] shortcode is dumping serialize($_SERVER), which contains all environment variables. The leakage occurs on all public facing pages containing the [accessally_order_form] shortcode, no login or administrator role is required.	2021-04-12	5	CVE-2021-24226 CONFIRM
atlassian -- data_center	The dashboard gadgets preference resource of the Atlassian gadgets plugin used in Jira Server and Jira Data Center before version 8.13.5, and from version 8.14.0 before version 8.15.1 allows remote anonymous attackers to obtain gadget related settings via a missing permissions check.	2021-04-09	5	CVE-2020-36287 MISC
dreamreport -- dream_report	A privilege escalation vulnerability exists in Dream Report 5 R20-2. COM Class Identifiers (CLSID), installed by Dream Report 5 20-2, reference LocalServer32 and InprocServer32 with weak privileges which can lead to privilege escalation when used. An attacker can provide a malicious file to trigger this vulnerability.	2021-04-09	6.8	CVE-2020-13534 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dreamreport -- dream_report	A privilege escalation vulnerability exists in Dream Report 5 R20-2. IIn the default configuration, the following registry keys, which reference binaries with weak permissions, can be abused by attackers to effectively ‘backdoor’ the installation files and escalate privileges when a new user logs in and uses the application.	2021-04-09	4.4	CVE-2020-13533 MISC
fortinet -- fortiadc	A clear text storage of sensitive information into log file vulnerability in FortiADCManager 5.3.0 and below, 5.2.1 and below and FortiADC 5.3.7 and below may allow a remote authenticated attacker to read other local users' password in log files.	2021-04-12	4	CVE-2021-24024 CONFIRM
google -- android	In onCreate of DeviceChooserActivity.java, there is a possible way to bypass user consent when pairing a Bluetooth device due to a tapjacking/overlay attack. This could lead to local escalation of privilege and pairing malicious devices with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-171221090	2021-04-13	5.4	CVE-2021-0433 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In several functions of InputDispatcher.cpp, WindowManagerService.java, and related files, there is a possible tapjacking attack due to an incorrect FLAG_OBSCURED value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10Android ID: A-152064592	2021-04-13	4.4	CVE-2021-0438 MISC
google -- android	In ClearPullerCacheIfNecessary and ForceClearPullerCache of StatsPullerManager.cpp, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-173552790	2021-04-13	4.4	CVE-2021-0432 MISC
google -- android	In updateInfo of android_hardware_input_InputApplicationHandle.cpp, there is a possible control of code flow due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	2021-04-13	4.6	CVE-2021-0442 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation.Product: AndroidVersions: Android-11Android ID: A-174768985			
google -- android	In setPowerModeWithHandle of com_android_server_power_PowerManagerService.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174243830	2021-04-13	4.6	CVE-2021-0439 MISC
google -- android	In setPlayPolicy of DrmPlugin.cpp, there is a possible double free. This could lead to local escalation of privilege in a privileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-176168330	2021-04-13	4.6	CVE-2021-0437 MISC
google -- android	In pollOnce of ALooper.cpp, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User	2021-04-13	4.6	CVE-2021-0429 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-175074139			
google -- android	In parsePrimaryFieldFirstUidAnnotation of LogEvent.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174485572	2021-04-13	4.6	CVE-2021-0426 MISC
google -- android	In avrc_proc_vendor_command of avrc_api.cc, there is a possible leak of heap data due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174150451	2021-04-13	5	CVE-2021-0435 MISC
google -- android	In avrc_msg_cback of avrc_api.cc, there is a possible out of bounds read due to a missing	2021-04-13	5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bounds check. This could lead to remote information disclosure to a paired device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174149901			0431 MISC
google -- android	In parseExclusiveStateAnnotation of LogEvent.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174488848	2021-04-13	4.6	CVE-2021-0427 MISC
google -- chrome	Use after free in V8 in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-09	6.8	CVE-2021-21195 MISC MISC
google -- chrome	Use after free in screen sharing in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to	2021-04-09	6.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	potentially exploit heap corruption via a crafted HTML page.			21194 MISC MISC
google -- chrome	Heap buffer overflow in TabStrip in Google Chrome on Windows prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-09	6.8	CVE-2021-21196 MISC MISC
google -- chrome	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-09	6.8	CVE-2021-21197 MISC MISC
google -- chrome	Use after free in Aura in Google Chrome on Linux prior to 89.0.4389.114 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2021-04-09	6.8	CVE-2021-21199 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Out of bounds read in IPC in Google Chrome prior to 89.0.4389.114 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-04-09	4.3	CVE-2021-21198 MISC MISC
ibm -- collaborative_lifecycle_management	IBM Jazz Team Server products use weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 192422.	2021-04-12	5	CVE-2020-4965 XF CONFIRM
ibm -- collaborative_lifecycle_management	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441.	2021-04-12	4.3	CVE-2021-20519 XF CONFIRM
ibm -- collaborative_lifecycle_management	IBM Jazz Team Server products contain an undisclosed vulnerability that could allow an authenticated user to present a customized message	2021-04-12	4	CVE-2020-4964 XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	on the application which could be used to phish other users. IBM X-Force ID: 192419.			CONFIRM
ibm -- collaborative_lifecycle_management	IBM Jazz Team Server products are vulnerable to stored 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: 191396.	2021-04-12	4.3	CVE-2020-4920 XF CONFIRM
intelliants -- subrion	Cross Site Scripting (XSS) vulnerability in subrion CMS Version <= 4.2.1 allows remote attackers to execute arbitrary web script via the "payment gateway" column on transactions tab.	2021-04-09	4.3	CVE-2020-23761 MISC MISC
libsixel_project -- libsixel	Buffer Overflow in the "sixel_encoder_encode_bytes" function of Libsixel v1.8.6 allows attackers to cause a Denial of Service (DoS).	2021-04-14	5	CVE-2020-36120 MISC
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2.	2021-04-09	4	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Special:Contributions can leak that a "hidden" user exists.			30156 MISC
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.31.13 and 1.32.x through 1.35.x before 1.35.2. When using the MediaWiki API to "protect" a page, a user is currently able to protect to a higher level than they currently have permissions for.	2021-04-09	4	CVE-2021-30152 MISC DEBIAN
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. ContentModelChange does not check if a user has correct permissions to create and set the content model of a nonexistent page.	2021-04-09	4	CVE-2021-30155 MISC DEBIAN
microsoft -- team_foundation_server	Azure DevOps Server and Team Foundation Server Information Disclosure Vulnerability	2021-04-13	4	CVE-2021-27067 MISC
microsoft -- visual_studio	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID	2021-04-13	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	is unique from CVE-2021-28313, CVE-2021-28322.			28321 MISC
microsoft -- visual_studio	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28321, CVE-2021-28322.	2021-04-13	4.6	CVE-2021-28313 MISC
microsoft -- visual_studio	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28313, CVE-2021-28321.	2021-04-13	4.6	CVE-2021-28322 MISC
microsoft -- visual_studio_2017	Visual Studio Installer Elevation of Privilege Vulnerability	2021-04-13	4.6	CVE-2021-27064 MISC
microsoft -- visual_studio_code	Visual Studio Code Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28457, CVE-2021-28469, CVE-2021-28473, CVE-2021-28475.	2021-04-13	6.8	CVE-2021-28477 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- visual_studio_code	Visual Studio Code Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28457, CVE-2021-28469, CVE-2021-28473, CVE-2021-28477.	2021-04-13	6.8	CVE-2021-28475 MISC
microsoft -- visual_studio_code	Visual Studio Code Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28457, CVE-2021-28469, CVE-2021-28475, CVE-2021-28477.	2021-04-13	6.8	CVE-2021-28473 MISC
microsoft -- windows_10	Windows Application Compatibility Cache Denial of Service Vulnerability	2021-04-13	4.3	CVE-2021-28311 MISC
microsoft -- windows_10	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability	2021-04-13	4.6	CVE-2021-28320 MISC
microsoft -- windows_10	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-27095.	2021-04-13	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				28315 MISC
microsoft -- windows_10	Windows Hyper-V Elevation of Privilege Vulnerability	2021-04-13	4.6	CVE-2021-28314 MISC
microsoft -- windows_10	Windows NTFS Denial of Service Vulnerability	2021-04-13	4.3	CVE-2021-28312 MISC
microsoft -- windows_10	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-27072.	2021-04-13	4.6	CVE-2021-28310 MISC
microsoft -- windows_10	NTFS Elevation of Privilege Vulnerability	2021-04-13	4.6	CVE-2021-27096 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	2021-04-13	4.6	CVE-2021-27090 MISC
microsoft -- windows_10	Windows AppX Deployment Server Denial of Service Vulnerability	2021-04-13	4.3	CVE-2021-28326 MISC
microsoft -- windows_10	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28328.	2021-04-13	4	CVE-2021-28323 MISC
microsoft -- windows_10	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28324.	2021-04-13	4	CVE-2021-28325 MISC
microsoft -- windows_10	Windows Event Tracing Elevation of Privilege Vulnerability	2021-04-13	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				27088 MISC
microsoft -- windows_10	Windows Services and Controller App Elevation of Privilege Vulnerability	2021-04-13	4.6	CVE-2021-27086 MISC MISC
microsoft -- windows_10	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28310.	2021-04-13	4.6	CVE-2021-27072 MISC
microsoft -- windows_10	Microsoft Internet Messaging API Remote Code Execution Vulnerability	2021-04-13	6.8	CVE-2021-27089 MISC
microsoft -- windows_10	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332,	2021-04-13	6.5	CVE-2021-28434 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358.			
microsoft -- windows_10	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28434.	2021-04-13	6.5	CVE-2021-28358 MISC
microsoft -- windows_10	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-	2021-04-13	6.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28358, CVE-2021-28434.			28357 MISC
microsoft -- windows_10	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434.	2021-04-13	6.5	CVE-2021-28356 MISC
microsoft -- windows_10	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique	2021-04-13	6.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434.			28355 MISC
microsoft -- windows_10	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28315.	2021-04-13	6.8	CVE-2021-27095 MISC
microsoft -- windows_10	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-	2021-04-13	6.5	CVE-2021-28354 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434.			
microsoft -- windows_10	Windows Media Photo Codec Information Disclosure Vulnerability	2021-04-13	6.3	CVE-2021-27079 MISC
microsoft -- windows_10	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28439.	2021-04-13	5	CVE-2021-28319 MISC
microsoft -- windows_10	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28325.	2021-04-13	5	CVE-2021-28324 MISC
microsoft -- windows_10	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332,	2021-04-13	6.5	CVE-2021-28353 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434.			
microsoft -- windows_10	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434.	2021-04-13	6.5	CVE-2021-28352 MISC
microsoft -- windows_10	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-	2021-04-13	6.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434.			28346 MISC
microsoft -- windows_10	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28440.	2021-04-13	4.6	CVE-2021-26415 MISC MISC
microsoft -- windows_7	RPC Endpoint Mapper Service Elevation of Privilege Vulnerability	2021-04-13	4.6	CVE-2021-27091 MISC
open-emr -- openemr	SQL injection vulnerability exists in phpGACL 3.3.7. A specially crafted HTTP request can lead to a SQL injection. An attacker can send an HTTP	2021-04-13	6.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	request to trigger this vulnerability in admin/edit_group.php, when the POST parameter action is “Submit”, the POST parameter parent_id leads to a SQL injection.			13568 MISC
open-emr -- openemr	SQL injection vulnerabilities exist in phpGACL 3.3.7. A specially crafted HTTP request can lead to a SQL injection. An attacker can send an HTTP request to trigger this vulnerability In admin/edit_group.php, when the POST parameter action is “Delete”, the POST parameter delete_group leads to a SQL injection.	2021-04-13	6.5	CVE-2020-13566 MISC
patreon -- patreon_wordpress	The Jetpack Scan team identified a Local File Disclosure vulnerability in the Patreon WordPress plugin before 1.7.0 that could be abused by anyone visiting the site. Using this attack vector, an attacker could leak important internal files like wp-config.php, which contains database credentials and cryptographic keys used in the generation of nonces and cookies.	2021-04-12	5	CVE-2021-24227 MISC CONFIRM
patreon -- patreon_wordpress	The Jetpack Scan team identified a Cross-Site Request Forgery vulnerability in the Patreon	2021-04-12	5.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WordPress plugin before 1.7.0, allowing attackers to make a logged in user overwrite or create arbitrary user metadata on the victim's account once visited. If exploited, this bug can be used to overwrite the "wp_capabilities" meta, which contains the affected user account's roles and privileges. Doing this would essentially lock them out of the site, blocking them from accessing paid content.			24230 MISC CONFIRM
patreon -- patreon_wordpress	The Jetpack Scan team identified a Reflected Cross-Site Scripting in the Login Form of the Patreon WordPress plugin before 1.7.2. The WordPress login form (wp-login.php) is hooked by the plugin and offers to allow users to authenticate on the site using their Patreon account. Unfortunately, some of the error logging logic behind the scene allowed user-controlled input to be reflected on the login page, unsanitized.	2021-04-12	6.8	CVE-2021-24228 MISC CONFIRM
patreon -- patreon_wordpress	The Jetpack Scan team identified a Cross-Site Request Forgery vulnerability in the Patreon WordPress plugin before 1.7.0, allowing attackers to make a logged administrator disconnect the site from Patreon by visiting a specially crafted link.	2021-04-12	4.3	CVE-2021-24231 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
patreon -- patreon_wordpress	The Jetpack Scan team identified a Reflected Cross-Site Scripting via the patreon_save_attachment_patreon_level AJAX action of the Patreon WordPress plugin before 1.7.2. This AJAX hook is used to update the pledge level required by Patreon subscribers to access a given attachment. This action is accessible for user accounts with the 'manage_options' privilege (i.e.., only administrators). Unfortunately, one of the parameters used in this AJAX endpoint is not sanitized before being printed back to the user, so the risk it represents is the same as the previous XSS vulnerability.	2021-04-12	6.8	CVE-2021-24229 MISC CONFIRM
perforce -- helix_alm	XML External Entity Resolution (XXE) in Helix ALM. The XML Import functionality of the Administration console in Perforce Helix ALM 2020.3.1 Build 22 accepts XML input data that is parsed by insecurely configured software components, leading to XXE attacks.	2021-04-13	6.4	CVE-2021-29997 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rukovoditel -- project_management	An exploitable SQL injection vulnerability exists in the "forms_fields_rules/rules" page of the Rukovoditel Project Management App 2.7.2. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability, this can be done either with administrator credentials or through cross-site request forgery.	2021-04-09	6.8	CVE-2020-13587 MISC
rukovoditel -- project_management	An exploitable SQL injection vulnerability exists in the "access_rules/rules_form" page of the Rukovoditel Project Management App 2.7.2. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability, this can be done either with administrator credentials or through cross-site request forgery.	2021-04-09	6.8	CVE-2020-13591 MISC
rukovoditel -- project_management	An exploitable SQL injection vulnerability exists in "global_lists/choices" page of the Rukovoditel Project Management App 2.7.2. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability, this can be done either	2021-04-09	6.8	CVE-2020-13592 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with administrator credentials or through cross-site request forgery.			
skyworthdigital -- rn510_firmware	Skyworth Digital Technology RN510 V.3.1.0.4 contains a cross-site request forgery (CSRF) vulnerability in /cgi-bin/net-routeadd.asp and /cgi-bin/sec-urlfilter.asp. Missing CSRF protection in devices can lead to XSRF, as the above pages are vulnerable to cross-site scripting (XSS).	2021-04-09	4.3	CVE-2021-25327 MISC
skyworthdigital -- rn510_firmware	Skyworth Digital Technology RN510 V.3.1.0.4 RN510 V.3.1.0.4 contains a buffer overflow vulnerability in /cgi-bin/app-staticIP.asp. An authenticated attacker can send a specially crafted request to endpoint which can lead to a denial of service (DoS) or possible code execution on the device.	2021-04-09	6.5	CVE-2021-25328 MISC
sonicwall -- email_security	SonicWall Email Security version 10.0.9.x contains a vulnerability that allows a post-authenticated attacker to upload an arbitrary file to the remote host.	2021-04-09	6.5	CVE-2021-20022 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tms-outsource -- wpdatatables	The wpDataTables – Tables & Table Charts premium WordPress plugin before 3.4.2 has Improper Access Control. A low privilege authenticated user that visits the page where the table is published can tamper the parameters to access the data of another user that are present in the same table by taking over the user permissions on the table through formdata[wdt_ID] parameter. By exploiting this issue an attacker is able to access and manage the data of all users in the same table.	2021-04-12	5.5	CVE-2021-24197 MISC MISC CONFIRM
tms-outsource -- wpdatatables	The wpDataTables – Tables & Table Charts premium WordPress plugin before 3.4.2 has Improper Access Control. A low privilege authenticated user that visits the page where the table is published can tamper the parameters to delete the data of another user that are present in the same table through id_key and id_val parameters. By exploiting this issue an attacker is able to delete the data of all users in the same table.	2021-04-12	5.5	CVE-2021-24198 MISC MISC CONFIRM
tms-outsource -- wpdatatables	The wpDataTables – Tables & Table Charts premium WordPress plugin before 3.4.2 allows a low privilege authenticated user to perform Boolean-based blind SQL Injection in the table list	2021-04-12	4	CVE-2021-24199 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	page on the endpoint /wp-admin/admin-ajax.php?action=get_wdtable&table_id=1, on the 'start' HTTP POST parameter. This allows an attacker to access all the data in the database and obtain access to the WordPress application.			MISC CONFIRM
tms-outsource -- wpdatatables	The wpDataTables – Tables & Table Charts premium WordPress plugin before 3.4.2 allows a low privilege authenticated user to perform Boolean-based blind SQL Injection in the table list page on the endpoint /wp-admin/admin-ajax.php?action=get_wdtable&table_id=1, on the 'length' HTTP POST parameter. This allows an attacker to access all the data in the database and obtain access to the WordPress application.	2021-04-12	4	CVE-2021-24200 MISC MISC CONFIRM
trendmicro -- password_manager	Trend Micro Password Manager version 5 (Consumer) is vulnerable to a DLL Hijacking vulnerability which could allow an attacker to inject a malicious DLL file during the installation progress and could execute a malicious program each time a user installs a program.	2021-04-13	4.4	CVE-2021-28647 N/A

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wikimedia -- parsoid	An issue was discovered in Wikimedia Parsoid before 0.11.1 and 0.12.x before 0.12.2. An attacker can send crafted wikitext that Utils/WTUtils.php will transform by using a <meta> tag, bypassing sanitization steps, and potentially allowing for XSS.	2021-04-09	4.3	CVE-2021-30458 MISC MISC
x2engine -- x2crm	Cross Site Scripting (XSS) in X2Engine X2CRM v6.9 and older allows remote attackers to execute arbitrary code by injecting arbitrary web script or HTML via the "New Name" field of the "Rename a Module" tool.	2021-04-14	4.3	CVE-2020-21087 MISC