Vulnerability Summary for the Week of June 7, 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
aomedia -- aomedia	aom_dsp/noise_model.c in libaom in AOMedia before 2021-03-24 has a buffer overflow.	2021-06-04	7.5	CVE-2021-30475 MISC MISC
broadcom -- sannav	Webtools in Brocade SANnav before version 2.1.1 allows unauthenticated users to make requests to arbitrary hosts due to a misconfiguration; this is commonly referred to as Server-Side Request Forgery (SSRF).	2021-06-09	7.5	CVE-2020-15377 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
chiyu-tech -- bf-430_firmware	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated.	2021-06-04	7.5	CVE-2021-31251 CONFIRM MISC MISC
linux -- linux_kernel	The eBPF RINGBUF bpf_ringbuf_reserve() function in the Linux kernel did not check that the allocated size was smaller than the ringbuf size, allowing an attacker to perform out-of-bounds writes within the kernel and therefore, arbitrary code execution. This issue was fixed via commit 4b81ccebaeee ("bpf, ringbuf: Deny reserve of buffers larger than ringbuf") (v5.13-rc4) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. It was introduced via 457f44363a88 ("bpf: Implement BPF ring buffer and verifier support for it") (v5.8-rc1).	2021-06-04	7.2	CVE-2021-3489 MISC UBUNTU UBUNTU MISC MLIST
linux -- linux_kernel	The eBPF ALU32 bounds tracking for bitwise ops (AND, OR and XOR) in the Linux kernel did not properly update 32-bit bounds, which could be turned into out of bounds reads and writes in the Linux kernel and therefore, arbitrary code execution. This issue was fixed via commit	2021-06-04	7.2	CVE-2021-3490 UBUNTU MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	049c4e13714e ("bpf: Fix alu32 const subreg bound tracking on bitwise operations") (v5.13-rc4) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. The AND/OR issues were introduced by commit 3f50f132d840 ("bpf: Verifier, do explicit ALU32 bounds tracking") (5.7-rc1) and the XOR variant was introduced by 2921c90d4718 ("bpf:Fix a verifier failure with xor") (5.10-rc1).			UBUNTU MLIST
linux -- linux_kernel	The io_uring subsystem in the Linux kernel allowed the MAX_RW_COUNT limit to be bypassed in the PROVIDE_BUFFERS operation, which led to negative values being usedin mem_rw when reading /proc/<PID>/mem. This could be used to create a heap overflow leading to arbitrary code execution in the kernel. It was addressed via commit d1f82808877b ("io_uring: truncate lengths larger than MAX_RW_COUNT on provide buffers") (v5.13-rc1) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. It was introduced in ddf0322db79c ("io_uring: add IORING_OP_PROVIDE_BUFFERS") (v5.7-rc1).	2021-06-04	7.2	CVE-2021-3491 UBUNTU UBUNTU MISC MISC MLIST
microsoft -- intune_management_extension	Microsoft Intune Management Extension Remote Code Execution Vulnerability	2021-06-08	7.5	CVE-2021-

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
				31980 MISC
microsoft -- windows_10	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31976.	2021-06-08	7.8	CVE-2021-31975 MISC
microsoft -- windows_10	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31975.	2021-06-08	7.8	CVE-2021-31976 MISC
microsoft -- windows_10	Kerberos AppContainer Security Feature Bypass Vulnerability	2021-06-08	7.5	CVE-2021-31962 MISC
qualcomm -- apq8009_firmware	Out of bound read will happen if EAPOL Key length is less than expected while processing NAN shared key descriptor attribute in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	2021-06-09	7.8	CVE-2020-11241 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking			

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accela -- civic_platform	In Accela Civic Platform through 21.1, the security/hostSignon.do parameter servProvCode is vulnerable to XSS.	2021-06-07	4.3	CVE-2021-33904 MISC MISC
adiscon -- loganalyzer	Adiscon LogAnalyzer 4.1.10 and 4.1.11 allow login.php XSS.	2021-06-08	4.3	CVE-2021-31738 MISC
bloofox -- bloofoxcms	BloofoxCMS 0.5.2.1 allows Directory traversal vulnerability by inserting '../' payloads within the 'fileurl' parameter.	2021-06-04	4	CVE-2020-36142 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bloofox -- bloofoxcms	BloofoxCMS 0.5.2.1 allows Unrestricted File Upload vulnerability via bypass MIME Type validation by inserting 'image/jpeg' within the 'Content-Type' header.	2021-06-04	6.5	CVE-2020-36141 MISC
bloofox -- bloofoxcms	BloofoxCMS 0.5.2.1 allows Cross-Site Request Forgery (CSRF) via 'mode=settings&page=editor', as demonstrated by use of 'mode=settings&page=editor' to change any file content (Locally/Remotely).	2021-06-04	4.3	CVE-2020-36140 MISC
broadcom -- sannav	Brocade SANNav before version 2.1.1 contains an information disclosure vulnerability. Successful exploitation of internal server information in the initial login response header.	2021-06-09	5	CVE-2020-15384 MISC
broadcom -- sannav	Brocade SANnav before version 2.1.1 logs account credentials at the ‘trace’ logging level.	2021-06-09	5	CVE-2020-15380 MISC
broadcom -- sannav	The OVA version of Brocade SANnav before version 2.1.1 installation with IPv6 networking exposes the docker container ports to the network, increasing the potential attack surface.	2021-06-09	5	CVE-2020-15378 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
broadcom -- sannav	Brocade SANnav before version 2.1.1 allows an authenticated attacker to list directories, and list files without permission. As a result, users without permission can see folders, and hidden files, and can create directories without permission.	2021-06-09	5.5	CVE-2020-15385 MISC
chiyu-tech -- bf-430_firmware	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it.	2021-06-04	5.8	CVE-2021-31252 CONFIRM MISC MISC
chiyu-tech -- bf-430_firmware	A CRLF injection vulnerability was found on BF-430, BF-431, and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of validation on the parameter redirect= available on multiple CGI components.	2021-06-04	6.4	CVE-2021-31249 MISC MISC MISC MISC
cisco -- webex_meetings_desktop	A vulnerability in Cisco Webex Meetings Desktop App for Windows, Cisco Webex Meetings Server, Cisco Webex Network Recording Player for Windows, and Cisco Webex Teams for Windows could allow an	2021-06-04	6.9	CVE-2021-1536 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated, local attacker to perform a DLL injection attack on an affected device. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. This vulnerability is due to incorrect handling of directory paths at run time. An attacker could exploit this vulnerability by inserting a configuration file in a specific path in the system, which can cause a malicious DLL file to be loaded when the application starts. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of another user account.			
ckeditor -- ckeditor	A cross-site scripting (XSS) vulnerability in the HTML Data Processor in CKEditor 4 4.14.0 through 4.16.x before 4.16.1 allows remote attackers to inject executable JavaScript code through a crafted comment because --!> is mishandled.	2021-06-09	4.3	CVE-2021-33829 MISC
cloverdx -- cloverdx	A cross-site scripting (XSS) vulnerability in CloverDX Server 5.9.0, CloverDX 5.8.1, CloverDX 5.7.0, and earlier allows remote attackers to inject arbitrary web script or HTML via the sessionToken parameter of multiple	2021-06-09	4.3	CVE-2021-30133 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	methods in Simple HTTP API. This is resolved in 5.9.1 and 5.10.			
dino -- dino	Dino before 0.1.2 and 0.2.x before 0.2.1 allows Directory Traversal (only for creation of new files) via URI-encoded path separators.	2021-06-07	5	CVE-2021-33896 CONFIRM MISC MLIST
dlink -- dir-868l_firmware	The D-Link router DIR-868L 3.01 is vulnerable to credentials disclosure in telnet service through decompilation of firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.	2021-06-04	5	CVE-2020-29321 MISC
dlink -- dir-880l_firmware	The D-Link router DIR-880L 1.07 is vulnerable to credentials disclosure in telnet service through decompilation of firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.	2021-06-04	5	CVE-2020-29322 MISC
dlink -- dir-885l-mfc_firmware	The D-link router DIR-885L-MFC 1.15b02, v1.21b05 is vulnerable to credentials disclosure in telnet service through decompilation of	2021-06-04	5	CVE-2020-

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.			29323 MISC
dlink -- dir-895l_mfc_firmware	The DLink Router DIR-895L MFC v1.21b05 is vulnerable to credentials disclosure in telnet service through decompilation of firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.	2021-06-04	5	CVE-2020-29324 MISC
entrouvert -- lasso	Lasso all versions prior to 2.7.0 has improper verification of a cryptographic signature.	2021-06-04	5	CVE-2021-28091 MISC MISC MISC DEBIAN MLIST FEDORA FEDORA
esri -- arcgis_server	A SQL injection vulnerability exists in some configurations of ArcGIS Server versions 10.8.1 and earlier. Specially crafted web requests can expose information that is not intended to be	2021-06-07	5	CVE-2021-29099 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disclosed (not customer datasets). Web Services that use file based data sources (file Geodatabase or Shape Files or tile cached services) are unaffected by this issue.			
gitlab -- gitlab	An issue has been discovered in GitLab affecting all versions starting with 13.10. GitLab was vulnerable to a stored XSS in blob viewer of notebooks.	2021-06-08	4.3	CVE-2021-22220 CONFIRM MISC MISC
google -- chrome	Type confusion in V8 in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30517 MISC MISC
google -- chrome	Insufficient policy enforcement in PopupBlocker in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass navigation restrictions via a crafted iframe.	2021-06-07	4.3	CVE-2021-30533 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2021-06-07	4.3	CVE-2021-30532 MISC MISC
google -- chrome	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2021-06-07	4.3	CVE-2021-30531 MISC MISC
google -- chrome	Use after free in Autofill in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30514 MISC MISC
google -- chrome	Type confusion in V8 in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30513 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Out of bounds read in Tab Groups in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted HTML page.	2021-06-04	5.8	CVE-2021-30511 MISC MISC
google -- chrome	Use after free in Notifications in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30512 MISC MISC
google -- chrome	Insufficient policy enforcement in cookies in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass cookie policy via a crafted HTML page.	2021-06-07	4.3	CVE-2021-30537 MISC MISC
google -- chrome	Out of bounds read in V8 in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page.	2021-06-07	5.8	CVE-2021-30536 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Insufficient policy enforcement in content security policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2021-06-07	5.8	CVE-2021-30539 MISC MISC
google -- chrome	Use after free in Aura in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30510 MISC MISC
google -- chrome	Out of bounds write in Tab Strip in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page and a crafted Chrome extension.	2021-06-04	6.8	CVE-2021-30509 MISC MISC
google -- chrome	Heap buffer overflow in Media Feeds in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to enable certain features in Chrome to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30508 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Inappropriate implementation in Offline in Google Chrome on Android prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30507 MISC MISC
google -- chrome	Incorrect security UI in Web App Installs in Google Chrome on Android prior to 90.0.4430.212 allowed an attacker who convinced a user to install a web application to inject scripts or HTML into a privileged page via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30506 MISC MISC
google -- chrome	Insufficient policy enforcement in iFrameSandbox in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2021-06-07	4.3	CVE-2021-30534 MISC MISC
google -- chrome	Insufficient policy enforcement in content security policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2021-06-07	4.3	CVE-2021-30538 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Heap buffer overflow in Reader Mode in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30518 MISC MISC
google -- chrome	Use after free in WebUI in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-06-07	6.8	CVE-2021-30527 MISC MISC
google -- chrome	Use after free in Payments in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious payments app to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30519 MISC MISC
google -- chrome	Use after free in Tab Strip in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30520 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Heap buffer overflow in Autofill in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.	2021-06-07	6.8	CVE-2021-30521 MISC MISC
google -- chrome	Use after free in WebAudio in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-06-07	6.8	CVE-2021-30522 MISC MISC MISC
google -- chrome	Use after free in WebRTC in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted SCTP packet.	2021-06-07	6.8	CVE-2021-30523 MISC MISC
google -- chrome	Use after free in TabStrip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-06-07	6.8	CVE-2021-30524 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Use after free in TabGroups in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-06-07	6.8	CVE-2021-30525 MISC MISC
google -- chrome	Out of bounds write in TabStrip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page.	2021-06-07	6.8	CVE-2021-30526 MISC MISC
google -- chrome	Use after free in WebAuthentication in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker who had compromised the renderer process of a user who had saved a credit card in their Google account to potentially exploit heap corruption via a crafted HTML page.	2021-06-07	6.8	CVE-2021-30528 MISC MISC
google -- chrome	Use after free in File API in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30515 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Use after free in Bookmarks in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-06-07	6.8	CVE-2021-30529 MISC MISC
google -- chrome	Double free in ICU in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-06-07	6.8	CVE-2021-30535 MISC MISC
google -- chrome	Use after free in Tab Strip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-06-07	6.8	CVE-2021-30542 MISC MISC
google -- chrome	Use after free in Tab Strip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-06-07	6.8	CVE-2021-30543 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Incorrect security UI in payments in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2021-06-07	4.3	CVE-2021-30540 MISC MISC
google -- chrome	Heap buffer overflow in History in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	6.8	CVE-2021-30516 MISC MISC
google -- chrome	Out of bounds memory access in WebAudio in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.	2021-06-07	6.8	CVE-2021-30530 MISC MISC
ibm -- datapower_gateway	IBM DataPower Gateway 10.0.0.0 through 10.0.1.0 and 2018.4.1.0 through 2018.4.1.14 stores sensitive information in GET request parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 193033.	2021-06-07	5	CVE-2020-5008 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- websphere_application_server_nd	IBM WebSphere Application Server Network Deployment 8.5 and 9.0 could allow a remote authenticated attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to read and delete arbitrary files on the system. IBM X-Force ID: 198435.	2021-06-07	6.5	CVE-2021-20517 CONFIRM XF
inverse -- sogo	SOGo 2.x before 2.4.1 and 3.x through 5.x before 5.1.1 does not validate the signatures of any SAML assertions it receives. Any actor with network access to the deployment could impersonate users when SAML is the authentication method. (Only versions after 2.0.5a are affected.)	2021-06-04	5	CVE-2021-33054 MISC MISC MISC
jnews -- jnews	The JNews WordPress theme before 8.0.6 did not sanitise the cat_id parameter in the POST request /?ajax-request=jnews (with action=jnews_build_mega_category_*), leading to a Reflected Cross-Site Scripting (XSS) issue.	2021-06-07	4.3	CVE-2021-24342 CONFIRM
luca-app -- luca	Luca through 1.7.4 on Android allows remote attackers to obtain sensitive information about COVID-19 tracking because requests related to	2021-06-04	5	CVE-2021-33838 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Check-In State occur shortly after requests for Phone Number Registration.			MISC MISC MISC
luca-app -- luca	The server in Luca through 1.1.14 allows remote attackers to cause a denial of service (insertion of many fake records related to COVID-19) because Phone Number data lacks a digital signature.	2021-06-04	5	CVE-2021-33840 MISC MISC
luca-app -- luca	Luca through 1.7.4 on Android allows remote attackers to obtain sensitive information about COVID-19 tracking because the QR code of a Public Location can be intentionally confused with the QR code of a Private Meeting.	2021-06-04	5	CVE-2021-33839 MISC MISC MISC MISC
microsoft -- 365_apps	Microsoft Office Graphics Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31940.	2021-06-08	6.8	CVE-2021-31941 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- 365_apps	Microsoft Office Graphics Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31941.	2021-06-08	6.8	CVE-2021-31940 MISC
microsoft -- 3d_viewer	3D Viewer Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31942.	2021-06-08	6.8	CVE-2021-31943 MISC
microsoft -- 3d_viewer	3D Viewer Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31943.	2021-06-08	6.8	CVE-2021-31942 MISC
microsoft -- 3d_viewer	3D Viewer Information Disclosure Vulnerability	2021-06-08	4.3	CVE-2021-31944 MISC
microsoft -- edge	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2021-06-08	5.1	CVE-2021-33741 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- kubernetes_tools	Microsoft VsCode Kubernetes Tools Extension Elevation of Privilege Vulnerability	2021-06-08	6.8	CVE-2021-31938 MISC
microsoft -- malware_protection_engine	Microsoft Defender Remote Code Execution Vulnerability	2021-06-08	6.8	CVE-2021-31985 MISC
microsoft -- paint_3d	Paint 3D Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31945, CVE-2021-31983.	2021-06-08	6.8	CVE-2021-31946 MISC MISC
microsoft -- paint_3d	Paint 3D Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31946, CVE-2021-31983.	2021-06-08	6.8	CVE-2021-31945 MISC MISC
microsoft -- sharepoint_enterprise_server	Microsoft SharePoint Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31963, CVE-2021-31966.	2021-06-08	6.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				26420 MISC
microsoft -- vp9_video_extensions	VP9 Video Extensions Remote Code Execution Vulnerability	2021-06-08	6.8	CVE-2021-31967 MISC
microsoft -- windows_10	Windows Remote Desktop ServicesÂ Denial of Service Vulnerability	2021-06-08	5	CVE-2021-31968 MISC
microsoft -- windows_10	Server for NFS Denial of Service Vulnerability	2021-06-08	5	CVE-2021-31974 MISC
microsoft -- windows_10	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2021-06-08	4.6	CVE-2021-31969 MISC
microsoft -- windows_10	Windows GPSVC Elevation of Privilege Vulnerability	2021-06-08	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				31973 MISC
microsoft -- windows_10	Windows HTML Platform Security Feature Bypass Vulnerability	2021-06-08	6.8	CVE-2021-31971 MISC
microsoft -- windows_server_2008	Windows DCOM Server Security Feature Bypass	2021-06-08	4.3	CVE-2021-26414 MISC
microsoft -- windows_server_2008	Microsoft Enhanced Cryptographic Provider Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31199.	2021-06-08	4.6	CVE-2021-31201 MISC
microsoft -- windows_server_2008	Windows Print Spooler Elevation of Privilege Vulnerability	2021-06-08	6.8	CVE-2021-1675 MISC
openexr -- openexr	An integer overflow leading to a heap-buffer overflow was found in the DwaCompressor of OpenEXR in versions before 3.0.1. An attacker	2021-06-08	4.3	CVE-2021-23215

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could use this flaw to crash an application compiled with OpenEXR.			FEDORA MISC
openexr -- openexr	An integer overflow leading to a heap-buffer overflow was found in the DwaCompressor of OpenEXR in versions before 3.0.1. An attacker could use this flaw to crash an application compiled with OpenEXR. This is a different flaw from CVE-2021-23215.	2021-06-08	4.3	CVE-2021-26260 FEDORA MISC
openexr -- openexr	An integer overflow leading to a heap-buffer overflow was found in OpenEXR in versions before 3.0.1. An attacker could use this flaw to crash an application compiled with OpenEXR.	2021-06-08	4.3	CVE-2021-26945 MISC
openexr -- openexr	A heap-buffer overflow was found in the copyIntoFrameBuffer function of OpenEXR in versions before 3.0.1. An attacker could use this flaw to execute arbitrary code with the permissions of the user running the application compiled against OpenEXR.	2021-06-08	6.8	CVE-2021-23169 FEDORA MISC FEDORA
openvpn -- openvpn_access_server	OpenVPN Access Server 2.7.3 to 2.8.7 allows remote attackers to trigger an assert during the user authentication phase via incorrect	2021-06-04	5	CVE-2020-36382

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authentication token data in an early phase of the user authentication resulting in a denial of service.			MISC MISC
pagelayer -- pagelayer	PageLayer before 1.3.5 allows reflected XSS via the font-size parameter.	2021-06-07	4.3	CVE-2020-36383 MISC
pagelayer -- pagelayer	PageLayer before 1.3.5 allows reflected XSS via color settings.	2021-06-07	4.3	CVE-2020-36384 MISC
qualcomm -- apq8009_firmware	Time-of-check time-of-use race condition While processing partition entries due to newly created buffer was read again from mmc without validation in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-06-09	6.9	CVE-2020-11233 CONFIRM
qualcomm -- apq8009w_firmware	Use after free due to race condition when reopening the device driver repeatedly in	2021-06-09	6.9	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			11250 CONFIRM
qualcomm -- apq8096au_firmware	Resource leakage issue during dci client registration due to reference count is not decremented if dci client registration fails in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-06-09	4.6	CVE-2020-11160 CONFIRM
refined-github_project -- refined-github	The Refined GitHub browser extension before 21.6.8 might allow XSS via a link in a document. NOTE: github.com sends Content-Security-Policy headers to, in general, address XSS and other concerns.	2021-06-09	4.3	CVE-2021-34364 MISC MISC
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts	2021-06-09	4.3	CVE-2021-33661 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the application, this is caused due to Improper Input Validation.			
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated FLI file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	2021-06-09	4.3	CVE-2021-33660 MISC MISC
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated GIF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	2021-06-09	4.3	CVE-2021-33659 MISC MISC
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated TIF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	2021-06-09	4.3	CVE-2021-27641 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated JT file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	2021-06-09	4.3	CVE-2021-27638 MISC MISC
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated JT file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	2021-06-09	4.3	CVE-2021-27639 MISC MISC
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PSD file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	2021-06-09	4.3	CVE-2021-27640 MISC MISC
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file	2021-06-09	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.			27642 MISC MISC
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated IFF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	2021-06-09	4.3	CVE-2021-27643 MISC MISC
simple-log_project -- simple-log	Cross Site Request Forgery (CSRF) in Simple-Log v1.6 allows remote attackers to gain privilege and execute arbitrary code via the component "Simple-Log/admin/admin.php?act=act_add_member".	2021-06-07	6.8	CVE-2020-18265 MISC
simple-log_project -- simple-log	Cross Site Request Forgery (CSRF) in Simple-Log v1.6 allows remote attackers to gain privilege and execute arbitrary code via the component "Simple-Log/admin/admin.php?act=act_edit_member".	2021-06-07	6.8	CVE-2020-18264 MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
tracefinanacial -- crestbridge	Trace Financial CRESTBridge <6.3.0.02 contains an authenticated SQL injection vulnerability, which was fixed in 6.3.0.03.	2021-06-10	6.5	CVE-2020-24667 MISC MISC
tracefinanacial -- crestbridge	Trace Financial CRESTBridge <6.3.0.02 contains an authenticated SQL injection vulnerability, which was fixed in 6.3.0.03.	2021-06-10	6.5	CVE-2020-24671 MISC MISC
wireshark -- wireshark	Infinite loop in DVB-S2-BB dissector in Wireshark 3.4.0 to 3.4.5 allows denial of service via packet injection or crafted capture file	2021-06-07	5	CVE-2021-22222 CONFIRM MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bloofox -- bloofoxcms	BloofoxCMS 0.5.2.1 allows Reflected Cross-Site Scripting (XSS) vulnerability by inserting a XSS payload within the 'fileurl' parameter.	2021-06-04	3.5	CVE-2020-36139 MISC
chiyu-tech -- bf-430_firmware	Multiple storage XSS vulnerabilities were discovered on BF-430, BF-431 and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of sanitization of the input on the components man.cgi, if.cgi, dhcpc.cgi, ppp.cgi.	2021-06-04	3.5	CVE-2021-31250 MISC MISC MISC
iflychat -- iflychat	The iFlyChat - WordPress Chat plugin through 4.6.4 does not sanitise its APP ID setting before outputting it back in the page, leading to an authenticated Stored Cross-Site Scripting issue	2021-06-07	3.5	CVE-2021-24343 CONFIRM
microsoft -- malware_protection_engine	Microsoft Defender Denial of Service Vulnerability	2021-06-08	2.1	CVE-2021-31978 MISC
microsoft -- windows_10	Windows Kernel Information Disclosure Vulnerability	2021-06-08	2.1	CVE-2021-

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
				31955 MISC
microsoft -- windows_10	Windows Bind Filter Driver Information Disclosure Vulnerability	2021-06-08	2.1	CVE-2021-31960 MISC
microsoft -- windows_10	Windows TCP/IP Driver Security Feature Bypass Vulnerability	2021-06-08	2.1	CVE-2021-31970 MISC
microsoft -- windows_10	Event Tracing for Windows Information Disclosure Vulnerability	2021-06-08	2.1	CVE-2021-31972 MISC
openvpn -- openvpn_access_server	OpenVPN Access Server 2.8.7 and earlier versions allows a remote attackers to bypass authentication and access control channel data on servers configured with deferred authentication, which can be used to potentially trigger further information leaks.	2021-06-04	3.5	CVE-2020-15077 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tracefinanacial -- crestbridge	Trace Financial CRESTBridge <6.3.0.02 contains a stored XSS vulnerability, which was fixed in 6.3.0.03.	2021-06-10	3.5	CVE-2020-24663 MISC MISC
tracefinancial -- crestbridge	Trace Financial Crest Bridge <6.3.0.02 contains a stored XSS vulnerability, which was fixed in 6.3.0.03.	2021-06-10	3.5	CVE-2020-24668 MISC MISC