Vulnerability Summary for the Week of June 21, 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
apache -- nuttx	Apache Nuttx Versions prior to 10.1.0 are vulnerable to integer wrap-around in functions malloc, realloc and memalign. This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	2021-06-21	7.5	CVE-2021-26461 CONFIRM
autoptimize -- autoptimize	The Autoptimize WordPress plugin before 2.7.8 attempts to delete malicious files (such as .php) form the uploaded archive via the "Import Settings" feature, after its extraction. However, the extracted folders are not checked and it is possible to upload a	2021-06-21	7.5	CVE-2021-24376 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	zip which contained a directory with PHP file in it and then it is not removed from the disk. It is a bypass of CVE-2020-24948 which allows sending a PHP file via the "Import Settings" functionality to achieve Remote Code Execution.			
ayecode -- location_manager	In the Location Manager WordPress plugin before 2.1.0.10, the AJAX action gd_popular_location_list did not properly sanitise or validate some of its POST parameters, which are then used in a SQL statement, leading to unauthenticated SQL Injection issues.	2021-06-21	7.5	CVE-2021-24361 MISC CONFIRM
cleo -- lexicom	An issue was discovered in Cleo LexiCom 5.5.0.0. Within the AS2 message, the sender can specify a filename. This filename can include path-traversal characters, allowing the file to be written to an arbitrary location on disk.	2021-06-18	7.5	CVE-2021-33576 MISC MISC
contiki-ng -- contiki-ng	Contiki-NG is an open-source, cross-platform operating system for internet of things devices. A buffer overflow vulnerability exists in Contiki-NG versions prior to 4.6. After establishing a TCP socket using the tcp-socket library, it is possible for the remote end to send a packet with a data offset that is unvalidated. The problem has been patched in	2021-06-18	7.5	CVE-2021-21281 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Contiki-NG 4.6. Users can apply the patch for this vulnerability out-of-band as a workaround.			
contiki-ng -- contiki-ng	Contiki-NG is an open-source, cross-platform operating system for internet of things devices. It is possible to cause an out-of-bounds write in versions of Contiki-NG prior to 4.6 when transmitting a 6LoWPAN packet with a chain of extension headers. Unfortunately, the written header is not checked to be within the available space, thereby making it possible to write outside the buffer. The problem has been patched in Contiki-NG 4.6. Users can apply the patch for this vulnerability out-of-band as a workaround.	2021-06-18	7.5	CVE-2021-21280 MISC CONFIRM
contiki-ng -- contiki-ng	Contiki-NG is an open-source, cross-platform operating system for internet of things devices. In verions prior to 4.6, an attacker can perform a denial-of-service attack by triggering an infinite loop in the processing of IPv6 neighbor solicitation (NS) messages. This type of attack can effectively shut down the operation of the system because of the cooperative scheduling used for the main parts of Contiki-NG and its communication stack. The problem has been patched in Contiki-NG 4.6. Users can apply the patch for this vulnerability out-of-band as a workaround.	2021-06-18	7.8	CVE-2021-21279 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
contiki-ng -- contiki-ng	Contiki-NG is an open-source, cross-platform operating system for internet of things devices. In versions prior to 4.5, buffer overflow can be triggered by an input packet when using either of Contiki-NG's two RPL implementations in source-routing mode. The problem has been patched in Contiki-NG 4.5. Users can apply the patch for this vulnerability out-of-band as a workaround.	2021-06-18	7.5	CVE-2021-21282 MISC CONFIRM
google -- android	In updateDrawable of StatusBarIconView.java, there is a possible permission bypass due to an uncaught exception. This could lead to local escalation of privilege by running foreground services without notifying the user, with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-169255797	2021-06-21	7.2	CVE-2021-0478 MISC
google -- android	In handle_rc_metamsg_cmd of btif_rc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth 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-181860042	2021-06-21	8.3	CVE-2021-0507 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In the Settings app, there is a possible way to disable an always-on VPN due to a missing permission 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-179975048	2021-06-21	7.2	CVE-2021-0505 MISC
google -- android	In p2p_process_prov_disc_req of p2p_pd.c, there is a possible out of bounds read and write due to a use after free. This could lead to remote escalation of privilege 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-181660448	2021-06-21	7.5	CVE-2021-0516 MISC
greenbone -- greenbone_security_assistant	Greenbone Security Assistant (GSA) before 7.0.3 and Greenbone OS (GOS) before 5.0.0 allow Host Header Injection.	2021-06-21	7.5	CVE-2018-25016 MISC MISC MISC
jenkins -- generic_webhook_trigger	Jenkins Generic Webhook Trigger Plugin 1.72 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2021-06-18	7.5	CVE-2021-21669

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM MLIST
joomla -- joomla\!	Joomla! Core is prone to a security bypass vulnerability. Exploiting this issue may allow attackers to perform otherwise restricted actions and subsequently retrieve password reset tokens from the database through an already existing SQL injection vector. Joomla! Core versions 1.5.x ranging from 1.5.0 and up to and including 1.5.15 are vulnerable.	2021-06-21	7.5	CVE-2010-1435 MISC MISC
joomla -- joomla\!	Joomla! Core is prone to a vulnerability that lets attackers upload arbitrary files because the application fails to properly verify user-supplied input. An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation; other attacks are also possible. Joomla! Core versions 1.5.x ranging from 1.5.0 and up to and including 1.5.15 are vulnerable.	2021-06-21	7.5	CVE-2010-1433 MISC MISC
primion-digitek -- secure_8	Secure 8 (Evalos) does not validate user input data correctly, allowing a remote attacker to perform a Blind SQL Injection. An attacker could exploit this vulnerability in order to extract information of users and administrator accounts stored in the database.	2021-06-18	7.5	CVE-2021-3604 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
radykal -- fancy_product_designer	The Fancy Product Designer WordPress plugin before 4.6.9 allows unauthenticated attackers to upload arbitrary files, resulting in remote code execution.	2021-06-21	7.5	CVE-2021-24370 MISC CONFIRM
serenityos -- serenityos	SerenityOS before commit 3844e8569689dd476064a0759d704bc64fb3ca2c contains a directory traversal vulnerability in tar/unzip that may lead to command execution or privilege escalation.	2021-06-18	7.5	CVE-2021-31272 MISC MISC MISC CONFIRM
textpattern -- textpattern	Textpattern 4.7.3 contains an aribtrary file load via the file_insert function in include/txp_file.php.	2021-06-21	7.5	CVE-2020-19510 MISC
txjia -- imcat	SQL Injection vulnerability in imcat v5.2 via the fm[auser] parameters in coms/add_coms.php.	2021-06-23	7.5	CVE-2020-20392 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
white_shark_systems_project -- white_shark_systems	White Shark System (WSS) 1.3.2 is vulnerable to unauthorized access via user_edit_password.php, remote attackers can modify the password of any user.	2021-06-21	7.5	CVE-2020-20466 MISC
white_shark_systems_project -- white_shark_systems	White Shark System (WSS) 1.3.2 has an unauthorized access vulnerability in default_user_edit.php, remote attackers can exploit this vulnerability to escalate to admin privileges.	2021-06-21	9	CVE-2020-20471 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
5none -- nonecms	Information Disclosure in NoneCMS v1.3 allows remote attackers to obtain sensitive information via the component "/nonecms/vendor".	2021-06-22	5	CVE-2020-18647 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
5none -- nonecms	Information Disclosure in NoneCMS v1.3 allows remote attackers to obtain sensitive information via the component "/public/index.php".	2021-06-22	5	CVE-2020-18646 MISC
accellion -- kiteworks	Accellion Kiteworks before 7.3.1 allows a user with Admin privileges to escalate their privileges by generating SSH passwords that allow local access.	2021-06-23	4.6	CVE-2021-31585 CONFIRM MISC
accellion -- kiteworks	Accellion Kiteworks before 7.4.0 allows an authenticated user to perform SQL Injection via LDAPGroup Search.	2021-06-23	6.5	CVE-2021-31586 MISC CONFIRM
advantech -- webaccess\/scada	Advantech WebAccess/SCADA Versions 9.0.1 and prior is vulnerable to a directory traversal, which may allow an attacker to remotely read arbitrary files on the file system.	2021-06-18	6.8	CVE-2021-32954 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
advantech -- webaccess\/scada	Advantech WebAccess/SCADA Versions 9.0.1 and prior is vulnerable to redirection, which may allow an attacker to send a maliciously crafted URL that could result in redirecting a user to a malicious webpage.	2021-06-18	5.8	CVE-2021-32956 MISC
akaunting -- akaunting	Akaunting <= 2.0.9 is vulnerable to CSV injection in the Item name field, export function. Attackers can inject arbitrary code into the name parameter and perform code execution when the crafted file is opened.	2021-06-21	6.8	CVE-2020-22390 MISC
automattic -- jetpack	The Jetpack Carousel module of the JetPack WordPress plugin before 9.8 allows users to create a "carousel" type image gallery and allows users to comment on the images. A security vulnerability was found within the Jetpack Carousel module by nguyenhg_vcs that allowed the comments of non-published page/posts to be leaked.	2021-06-21	5	CVE-2021-24374 CONFIRM MISC
autoptimize -- autoptimize	The Autoptimize WordPress plugin before 2.7.8 attempts to remove potential malicious files from the extracted archive uploaded via the 'Import Settings' feature, however this is not sufficient to protect against RCE as a race condition can be achieved in	2021-06-21	6.8	CVE-2021-24377 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	between the moment the file is extracted on the disk but not yet removed. It is a bypass of CVE-2020-24948.			
bosch -- b426_firmware	This vulnerability could allow an attacker to hijack a session while a user is logged in the configuration web page. This vulnerability was discovered by a security researcher in B426 and found during internal product tests in B426-CN/B429-CN, and B426-M and has been fixed already starting from version 3.08 on, which was released on June 2019.	2021-06-18	6.8	CVE-2021-23845 CONFIRM
bosch -- b426_firmware	When using http protocol, the user password is transmitted as a clear text parameter for which it is possible to be obtained by an attacker through a MITM attack. This will be fixed starting from Firmware version 3.11.5, which will be released on the 30th of June, 2021.	2021-06-18	4.3	CVE-2021-23846 CONFIRM
cleo -- lexicom	An issue was discovered in Cleo LexiCom 5.5.0.0. The requirement for the sender of an AS2 message to identify themselves (via encryption and signing of the message) can be bypassed by changing the Content-Type of the message to text/plain.	2021-06-18	5	CVE-2021-33577 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
collne -- welcart	Cross-site scripting vulnerability in Welcart e-Commerce versions prior to 2.2.4 allows remote attackers to inject arbitrary script or HTML via unspecified vectors.	2021-06-22	4.3	CVE-2021-20734 MISC MISC
color-string_project -- color-string	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in Color-String version 1.5.5 and below which occurs when the application is provided and checks a crafted invalid HWB string.	2021-06-21	5	CVE-2021-29060 MISC MISC MISC MISC
contiki-ng -- contiki-ng	Contiki-NG is an open-source, cross-platform operating system for internet of things devices. The RPL-Classic and RPL-Lite implementations in the Contiki-NG operating system versions prior to 4.6 do not validate the address pointer in the RPL source routing header This makes it possible for an attacker to cause out-of-bounds writes with packets injected into the network stack. Specifically, the problem lies in the rpl_ext_header_srh_update function in the two rpl-ext-header.c modules for RPL-Classic and RPL-Lite respectively. The addr_ptr variable is calculated	2021-06-18	5	CVE-2021-21257 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	using an unvalidated CMPR field value from the source routing header. An out-of-bounds write can be triggered on line 151 in os/net/routing/rpl-lite/rpl-ext-header.c and line 261 in os/net/routing/rpl-classic/rpl-ext-header.c, which contain the following memcpy call with addr_ptr as destination. The problem has been patched in Contiki-NG 4.6. Users can apply a patch out-of-band as a workaround.			
contiki-ng -- contiki-ng	Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. An out-of-bounds read can be triggered by 6LoWPAN packets sent to devices running Contiki-NG 4.6 and prior. The IPv6 header decompression function (<code>uncompress_hdr_iphc</code>) does not perform proper boundary checks when reading from the packet buffer. Hence, it is possible to construct a compressed 6LoWPAN packet that will read more bytes than what is available from the packet buffer. As of time of publication, there is not a release with a patch available. Users can apply the patch for this vulnerability out-of-band as a workaround.	2021-06-18	6.4	CVE-2021-21410 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ec-cube -- business_form_output	Cross-site scripting vulnerability in EC-CUBE Category contents plugin (for EC-CUBE 3.0 series) versions prior to version 1.0.1 allows a remote attacker to inject an arbitrary script by leading an administrator or a user to a specially crafted page and to perform a specific operation.	2021-06-22	4.3	CVE-2021-20744 MISC MISC
ec-cube -- business_form_output	Cross-site scripting vulnerability in EC-CUBE Business form output plugin (for EC-CUBE 3.0 series) versions prior to version 1.0.1 allows a remote attacker to inject an arbitrary script via unspecified vector.	2021-06-22	4.3	CVE-2021-20742 MISC MISC
ec-cube -- email_newsletters_management	Cross-site scripting vulnerability in EC-CUBE Email newsletters management plugin (for EC-CUBE 3.0 series) versions prior to version 1.0.4 allows a remote attacker to inject an arbitrary script by leading a user to a specially crafted page and to perform a specific operation.	2021-06-22	4.3	CVE-2021-20743 MISC MISC
expresstech -- quiz_and_survey_master	The Quiz And Survey Master â€“ Best Quiz, Exam and Survey Plugin WordPress plugin before 7.1.18 did not sanitise or escape its result_id parameter when displaying an existing quiz result page, leading to a	2021-06-20	4.3	CVE-2021-24368

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	reflected Cross-Site Scripting issue. This could allow for privilege escalation by inducing a logged in admin to open a malicious link			CONFIRM
get-simple -- getsimplecms	Cross Site Scriptiong (XSS) vulnerability in GetSimpleCMS <=3.3.15 via the timezone parameter to settings.php.	2021-06-23	4.3	CVE-2020-18658 MISC MISC MISC
get-simple -- getsimplecms	Cross Site Scripting vulnerability in GetSimpleCMS <=3.3.15 via the (1) sitename, (2) username, and (3) email parameters to /admin/setup.php	2021-06-23	4.3	CVE-2020-18659 MISC MISC MISC
getastra -- wp_hardening	The WP Hardening â€“ Fix Your WordPress Security WordPress plugin before 1.2.2 did not sanitise or escape the $_SERVER['REQUEST_URI'] before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue.	2021-06-21	4.3	CVE-2021-24372 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
getastra -- wp_hardening	The WP Hardening â€“ Fix Your WordPress Security WordPress plugin before 1.2.2 did not sanitise or escape the historyvalue GET parameter before outputting it in a Javascript block, leading to a reflected Cross-Site Scripting issue.	2021-06-21	4.3	CVE-2021-24373 CONFIRM
gitpod -- gitpod	Gitpod before 0.6.0 allows unvalidated redirects.	2021-06-22	5.8	CVE-2021-35206 MISC MISC MISC MISC MISC MISC MISC MISC
google -- android	In archiveStoredConversation of MmsService.java, there is a possible way to archive message conversation without user consent due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	2021-06-22	4.6	CVE-2021-0539 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation.Product: AndroidVersions: Android-11Android ID: A-180419673			
google -- android	In dropFile of WiFiInstaller, there is a way to delete files accessible to CertInstaller due to a confused deputy. 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-176756691	2021-06-22	4.6	CVE-2021-0536 MISC
google -- android	In wpas_ctrl_msg_queue_timeout of ctrl_iface_unix.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-168314741	2021-06-22	4.6	CVE-2021-0535 MISC
google -- android	In halWrapperDataCallback of hal_wrapper.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	2021-06-22	4.6	CVE-2021-0540 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation.Product: AndroidVersions: Android-11Android ID: A-169328517			
google -- android	In RenderStruct of protostream_objectsource.cc, there is a possible crash due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179161711	2021-06-22	5	CVE-2021-0555 MISC
google -- android	In ConnectionHandler::SdpCb of connection_handler.cc, there is a possible out of bounds read due to a use after free. 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-9 Android-10Android ID: A-174182139	2021-06-21	5	CVE-2021-0522 MISC
google -- android	In ActivityPicker.java, there is a possible bypass of user interaction in intent resolution due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges	2021-06-21	6.9	CVE-2021-0506 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-181962311			
google -- android	In permission declarations of DeviceAdminReceiver.java, there is a possible lack of broadcast protection due to an insecure default value. 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-170639543	2021-06-22	4.6	CVE-2021-0534 MISC
google -- android	In memory management driver, there is a possible memory corruption 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 exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185195272	2021-06-21	4.6	CVE-2021-0531 MISC
google -- android	In memory management driver, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with no additional	2021-06-21	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185196175			0530 MISC
google -- android	In memory management driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185195268	2021-06-21	4.6	CVE-2021-0529 MISC
google -- android	In memory management driver, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185195266	2021-06-21	4.6	CVE-2021-0528 MISC
google -- android	In memory management driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not	2021-06-21	4.6	CVE-2021-0527 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185193931			
google -- android	In phNxpNciHal_process_ext_rsp of phNxpNciHal_ext.cc, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169258743	2021-06-22	4.6	CVE-2021-0543 MISC
google -- android	In memory management driver, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185195264	2021-06-21	4.6	CVE-2021-0526 MISC
google -- android	In memory management driver, there is a possible out of bounds write 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 exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185193929	2021-06-21	4.6	CVE-2021-0525 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In deleteNotificationChannel and related functions of NotificationManagerService.java, there is a possible permission bypass due to improper state validation. This could lead to local escalation of privilege via hidden services with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-156090809	2021-06-21	4.6	CVE-2021-0513 MISC
google -- android	In __hidinput_change_resolution_multipliers of hid-input.c, 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 kernelAndroid ID: A-173843328References: Upstream kernel	2021-06-21	4.6	CVE-2021-0512 MISC
google -- android	In Dex2oat of dex2oat.cc, there is a possible way to inject bytecode into an app due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	2021-06-21	4.6	CVE-2021-0511 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11Android ID: A-178055795			
google -- android	In pfkey_dump of af_key.c, there is a possible out-of-bounds read due to a missing bounds check. This could lead to local information disclosure in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-110373476	2021-06-22	4.9	CVE-2021-0605 MISC
google -- android	In updateCapabilities of ConnectivityService.java, there is a possible incorrect network state determination due to a logic error in the code. This could lead to biasing of networking tasks to occur on non-VPN networks, which could lead to remote information disclosure, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179053823	2021-06-21	5	CVE-2021-0517 MISC
google -- android	In sendBugreportNotification of BugreportProgressService.java, there is a possible permission bypass due to an unsafe PendingIntent.	2021-06-22	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-178803845			0570 MISC
google -- android	In phNxpNciHal_print_res_status of phNxpNciHal.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169257710	2021-06-22	4.6	CVE-2021-0544 MISC
google -- android	In onCreate of WifiScanModeActivity.java, there is a possible way to enable Wi-Fi scanning without user consent due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-174047492	2021-06-21	4.4	CVE-2021-0523 MISC
google -- android	In bind of MediaControlPanel.java, there is a possible way to lock up the system UI using a malicious media	2021-06-22	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	file due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-180518039			0551 MISC
google -- android	In setRange of ABuffer.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179046129	2021-06-22	6.8	CVE-2021-0557 MISC
google -- android	In fillMainDataBuf of pvmp3_framedecoder.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-173473906	2021-06-22	4.3	CVE-2021-0558 MISC
google -- android	In Lag_max of p_ol_wgh.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no	2021-06-22	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172312730			0559 MISC
google -- android	In wrapUserThread of AudioStream.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-174801970	2021-06-22	4.4	CVE-2021-0565 MISC
google -- android	In decrypt of CryptoPlugin.cpp, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176495665	2021-06-22	4.4	CVE-2021-0564 MISC
google -- android	In onBindViewHolder of AppSwitchPreference.java, there is a possible bypass of device admin setttings due to unclear UI. This could lead to local escalation of privilege with User execution privileges needed.	2021-06-22	4.4	CVE-2021-0553 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169936038			
google -- android	In onCreate of EmergencyCallbackModeExitDialog.java, there is a possible exit of emergency callback mode due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-178821491	2021-06-22	4.4	CVE-2021-0538 MISC
google -- android	In onCreate of WiFiInstaller.java, there is a possible way to install a malicious Hotspot 2.0 configuration due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176756141	2021-06-22	4.4	CVE-2021-0537 MISC
google -- android	In memory management driver, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no	2021-06-21	4.4	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185193932			0533 MISC
google -- android	In memory management driver, there is a possible memory corruption 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 SoCAndroid ID: A-185196177	2021-06-21	4.4	CVE-2021-0532 MISC
google -- android	In several functions of MemoryFileSystem.cpp and related files, 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-11 Android-10Android ID: A-176237595	2021-06-21	4.4	CVE-2021-0520 MISC
google -- android	In phNxpNciHal_print_res_status of phNxpNciHal.cc, there is a possible out of bounds write due to a missing bounds check. This could lead	2021-06-22	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to local escalation of privilege in the NFC server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169258884			0545 MISC
google -- android	In various functions of CryptoPlugin.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-9 Android-10 Android-11 Android-8.1Android ID: A-176444161	2021-06-21	4.4	CVE-2021-0509 MISC
google -- android	In handleAppLaunch of AppLaunchActivity.java, there is a possible arbitrary activity launch due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-174870704	2021-06-22	4.6	CVE-2021-0608 MISC
google -- android	In iaxxx_calc_i2s_div of iaxxx-codec.c, there is a possible hardware port write with user controlled data	2021-06-22	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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 kernelAndroid ID: A-180950209			0607 MISC
google -- android	In drm_syncobj_handle_to_fd of drm_syncobj.c, there is a possible use after free due to incorrect refcounting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-168034487	2021-06-22	4.6	CVE-2021-0606 MISC
google -- android	In ActivityTaskManagerService.startActivity() and AppTaskImpl.startActivity() of ActivityTaskManagerService.java and AppTaskImpl.java, there is possible access to restricted activities due to a permissions bypass. 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-137395936	2021-06-22	4.6	CVE-2021-0571 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds write due to an integer 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-9 Android-10 Android-11 Android-8.1Android ID: A-176444622	2021-06-21	4.6	CVE-2021-0510 MISC
google -- android	In onReceive of DevicePolicyManagerService.java, there is a possible enabling of disabled profiles due to a missing permission 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-170121238	2021-06-22	4.6	CVE-2021-0568 MISC
google -- android	In isRestricted of RemoteViews.java, there is a possible way to inject font files due to a permissions bypass. 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-179461812	2021-06-22	4.6	CVE-2021-0567 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In onLoadFailed of AnnotateActivity.java, there is a possible way to gain WRITE_EXTERNAL_STORAGE permissions without user consent due to a confused deputy. 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-179688673	2021-06-22	4.6	CVE-2021-0550 MISC
google -- android	In rw_i93_send_to_lower of rw_i93.cc, 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-157650357	2021-06-22	4.6	CVE-2021-0548 MISC
google -- android	In onReceive of NetInitiatedActivity.java, there is a possible way to supply an attacker-controlled value to a GPS HAL handler due to a missing permission check. This could lead to local escalation of privilege that may result in undefined behavior in some HAL implementations with no additional execution privileges needed. User interaction is not needed for	2021-06-22	4.6	CVE-2021-0547 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation.Product: AndroidVersions: Android-11Android ID: A-174151048			
google -- android	In phNxpNciHal_print_res_status of phNxpNciHal.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169258733	2021-06-22	4.6	CVE-2021-0546 MISC
google -- android	In various functions of DrmPlugin.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-8.1 Android-9 Android-10 Android-11Android ID: A-176444154	2021-06-21	6.9	CVE-2021-0508 MISC
greenbone -- greenbone_security_assistant	Greenbone Security Assistant (GSA) before 8.0.2 and Greenbone OS (GOS) before 5.0.10 allow XSS during 404 URL handling in gsad.	2021-06-21	4.3	CVE-2019-25047 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
hisiphp -- hisiphp	Cross Site Scripting (XSS) vulnerability in HisiPHP 2.0.8 via the group name in addgroup.html.	2021-06-21	4.3	CVE-2020-21130 MISC
icehrm -- icehrm	A cross site request forgery (CSRF) vulnerability was discovered in Ice Hrm 29.0.0.OS which allows attackers to create new admin accounts or change users' passwords.	2021-06-22	6.8	CVE-2021-34244 MISC
icehrm -- icehrm	A session fixation vulnerability was discovered in Ice Hrm 29.0.0 OS which allows an attacker to hijack a valid user session via a crafted session cookie.	2021-06-22	5.8	CVE-2021-35046 MISC
icehrm -- icehrm	Cross site scripting (XSS) vulnerability in Ice Hrm 29.0.0.OS, allows attackers to execute arbitrary code via the parameters to the /app/ endpoint.	2021-06-22	4.3	CVE-2021-35045 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
increments -- qiita_markdown	Increments Qiita::Markdown before 0.34.0 allows XSS via a crafted gist link, a different vulnerability than CVE-2021-28796.	2021-06-21	4.3	CVE-2021-28833 MISC MISC
is-svg_project -- is-svg	A vulnerability was discovered in IS-SVG version 4.3.1 and below where a Regular Expression Denial of Service (ReDOS) occurs if the application is provided and checks a crafted invalid SVG string.	2021-06-21	5	CVE-2021-29059 MISC MISC MISC MISC
joomla -- joomla\!	Joomla! Core is prone to a session fixation vulnerability. An attacker may leverage this issue to hijack an arbitrary session and gain access to sensitive information, which may help in launching further attacks. Joomla! Core versions 1.5.x ranging from 1.5.0 and up to and including 1.5.15 are vulnerable.	2021-06-21	5	CVE-2010-1434 MISC MISC
joomla -- joomla\!	Joomla! Core is prone to an information disclosure vulnerability. Attackers can exploit this issue to obtain sensitive information that may help in	2021-06-21	5	CVE-2010-1432

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	launching further attacks. Joomla! Core versions 1.5.x ranging from 1.5.0 and up to and including 1.5.15 are vulnerable.			MISC MISC
juqingcms -- juqingcms	Cross Site Request Forgery (CSRF) in JuQingCMS v1.0 allows remote attackers to gain local privileges via the component "JuQingCMS_v1.0/admin/index.php?c=administrator&a=add".	2021-06-22	6.8	CVE-2020-18648 MISC
mcusystem -- mcusystem	The login page in the MCUsystem does not filter with special characters, which allows remote attackers can inject JavaScript without privilege and thus perform reflected XSS attacks.	2021-06-18	4.3	CVE-2021-32536 MISC
metinfo -- metinfo	Cross Site Scripting (XSS) vulnerability in MetInfo 7.0.0 via the gourl parameter in login.php.	2021-06-21	4.3	CVE-2020-21517 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
moxa -- mgate_mb3180_firmware	An issue was discovered on MOXA Mgate MB3180 Version 2.1 Build 18113012. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service.	2021-06-18	5	CVE-2021-33824 MISC MISC MISC
moxa -- mgate_mb3180_firmware	An issue was discovered on MOXA Mgate MB3180 Version 2.1 Build 18113012. Attacker could send a huge amount of TCP SYN packet to make web service's resource exhausted. Then the web server is denial-of-service.	2021-06-18	5	CVE-2021-33823 MISC MISC
mozilla -- firefox	Firefox for Android would become unstable and hard-to-recover when a website opened too many popups. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 89.	2021-06-24	4.3	CVE-2021-29962 MISC MISC
mozilla -- firefox	When drawing text onto a canvas with WebRender disabled, an out of bounds read could occur. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 89.0.1.	2021-06-24	5.8	CVE-2021-29968 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- firefox	Mozilla developers reported memory safety bugs present in Firefox 88. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 89.	2021-06-24	6.8	CVE-2021-29966 MISC MISC
mozilla -- firefox	When Web Render components were destructed, a race condition could have caused undefined behavior, and we presume that with enough effort may have been exploitable to run arbitrary code. This vulnerability affects Firefox < 88.0.1 and Firefox for Android < 88.1.3.	2021-06-24	5.1	CVE-2021-29952 MISC MISC
mozilla -- firefox	Mozilla developers and community members reported memory safety bugs present in Firefox 87. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 88.	2021-06-24	6.8	CVE-2021-29947 MISC MISC
mozilla -- firefox	Ports that were written as an integer overflow above the bounds of a 16-bit integer could have bypassed port blocking restrictions when used in the Alt-Svc	2021-06-24	6.8	CVE-2021-29946

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	header. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.			MISC MISC MISC MISC
mozilla -- firefox	When a download was initiated, the client did not check whether it was in normal or private browsing mode, which led to private mode cookies being shared in normal browsing mode. This vulnerability affects Firefox for iOS < 34.	2021-06-24	4.3	CVE-2021-29958 MISC MISC
mozilla -- firefox	Mozilla developers reported memory safety bugs present in Firefox 88 and Firefox ESR 78.11. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.11, Firefox < 89, and Firefox ESR < 78.11.	2021-06-24	6.8	CVE-2021-29967 MISC MISC MISC MISC
mozilla -- thunderbird	Thunderbird unprotects a secret OpenPGP key prior to using it for a decryption, signing or key import task. If the task runs into a failure, the secret key may remain in memory in its unprotected state. This vulnerability affects Thunderbird < 78.8.1.	2021-06-24	5	CVE-2021-29950 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mpmath -- mpmath	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in Mpmath v1.0.0 when the mpmathify function is called.	2021-06-21	5	CVE-2021-29063 MISC MISC MISC MISC
nvidia -- jetson_linux	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might allow an attacker to control all the RAM after the heap block, leading to denial of service or code execution.	2021-06-21	4.6	CVE-2021-34388 CONFIRM
openbsd -- openbsd	It was found in FreeBSD 8.0, 6.3 and 4.9, and OpenBSD 4.6 that a null pointer dereference in ftpd/popen.c may lead to remote denial of service of the ftpd service.	2021-06-22	5	CVE-2010-4816 MISC MISC MISC
owasp -- enterprise_security_api_for_java	It was found that all OWASP ESAPI for Java up to version 2.0 RC2 are vulnerable to padding oracle attacks.	2021-06-22	4.3	CVE-2010-3300

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\check_availability.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information.	2021-06-22	5	CVE-2020-22164 MISC
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\forgot-password.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information.	2021-06-22	5	CVE-2020-22166 MISC
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\user-login.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information.	2021-06-22	5	CVE-2020-22165 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\edit-profile.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information.	2021-06-22	5	CVE-2020-22173 MISC
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\admin\betweendates-detailsreports.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information.	2021-06-22	5	CVE-2020-22175 MISC
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\book-appointment.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information.	2021-06-22	5	CVE-2020-22174 MISC
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a sensitive information disclosure vulnerability in multiple areas. Remote unauthenticated users can exploit the vulnerability to obtain user sensitive information.	2021-06-22	5	CVE-2020-22176 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\get_doctor.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information.	2021-06-22	5	CVE-2020-22172 MISC
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\registration.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information.	2021-06-22	5	CVE-2020-22171 MISC
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\appointment-history.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information.	2021-06-22	5	CVE-2020-22169 MISC
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\change-emaild.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information.	2021-06-22	5	CVE-2020-22168 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a SQL injection vulnerability in \hms\get_doctor.php. Remote unauthenticated users can exploit the vulnerability to obtain database sensitive information.	2021-06-22	5	CVE-2020-22170 MISC
phpipam -- phpipam	phpIPAM 1.4.3 allows Reflected XSS via app/dashboard/widgets/ipcalc-result.php and app/tools/ip-calculator/result.php of the IP calculator.	2021-06-23	4.3	CVE-2021-35438 MISC
powerarchiver -- powerarchiver	The XML parser used in ConeXware PowerArchiver before 20.10.02 allows processing of external entities, which might lead to exfiltration of local files over the network (via an XXE attack).	2021-06-21	4.3	CVE-2021-28684 MISC MISC
prototypejs -- prototype	An issue was discovered in the stripTags and unescapeHTML components in Prototype 1.7.3 version 1.6 and below where an attacker can cause a Regular Expression Denial of Service (ReDOS) through stripping crafted HTML tags.	2021-06-21	5	CVE-2020-27511 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
riot-os -- riot	RIOT-OS 2021.01 before commit 85da504d2dc30188b89f44c3276fc5a25b31251f contains a buffer overflow which could allow attackers to obtain sensitive information.	2021-06-18	5	CVE-2021-31660 MISC CONFIRM
riot-os -- riot	RIOT-OS 2021.01 before commit 609c9ada34da5546cffb632a98b7ba157c112658 contains a buffer overflow that could allow attackers to obtain sensitive information.	2021-06-18	5	CVE-2021-31661 MISC CONFIRM
riot-os -- riot	RIOT-OS 2021.01 before commit 07f1254d8537497552e7dce80364aaead9266bbe contains a buffer overflow which could allow attackers to obtain sensitive information.	2021-06-18	5	CVE-2021-31662 CONFIRM MISC
riot-os -- riot	RIOT-OS 2021.01 before commit bc59d60be60dfc0a05def57d74985371e4f22d79	2021-06-18	5	CVE-2021-31663

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	contains a buffer overflow which could allow attackers to obtain sensitive information.			MISC MISC CONFIRM
riot-os -- riot	RIOT-OS 2021.01 before commit 44741ff99f7a71df45420635b238b9c22093647a contains a buffer overflow which could allow attackers to obtain sensitive information.	2021-06-18	5	CVE-2021-31664 MISC CONFIRM
serenityos -- serenityos	SerenityOS contains a buffer overflow in the set_range test in TestBitmap which could allow attackers to obtain sensitive information.	2021-06-18	5	CVE-2021-33185 CONFIRM
serenityos -- serenityos	SerenityOS in test-crypto.cpp contains a stack buffer overflow which could allow attackers to obtain sensitive information.	2021-06-18	5	CVE-2021-33186 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sing4g -- 4gee_router_hh70vb_firmware	An issue was discovered on 4GEE ROUTER HH70VB Version HH70_E1_02.00_22. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service.	2021-06-18	5	CVE-2021-33822 MISC MISC MISC
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager 3.x before 3.31.0 allows a remote authenticated attacker to get a list of blob files and read the content of a blob file (via a GET request) without having been granted access.	2021-06-18	4	CVE-2021-34553 CONFIRM
striptags_project -- striptags	The npm package "striptags" is an implementation of PHP's strip_tags in Typescript. In striptags before version 3.2.0, a type-confusion vulnerability can cause `striptags` to concatenate unsanitized strings when an array-like object is passed in as the `html` parameter. This can be abused by an attacker who can control the shape of their input, e.g. if query parameters are passed directly into the function. This can lead to a XSS.	2021-06-18	5	CVE-2021-32696 MISC MISC CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
synology -- calendar	Use of hard-coded credentials vulnerability in php component in Synology Calendar before 2.4.0-0761 allows remote attackers to obtain sensitive information via unspecified vectors.	2021-06-18	5	CVE-2021-34812 CONFIRM
synology -- download_station	Server-Side Request Forgery (SSRF) vulnerability in task management component in Synology Download Station before 3.8.16-3566 allows remote authenticated users to access intranet resources via unspecified vectors.	2021-06-18	4	CVE-2021-34811 CONFIRM
synology -- download_station	Improper privilege management vulnerability in cgi component in Synology Download Station before 3.8.16-3566 allows remote authenticated users to execute arbitrary code via unspecified vectors.	2021-06-18	6.5	CVE-2021-34810 CONFIRM
synology -- download_station	Improper neutralization of special elements used in a command ('Command Injection') vulnerability in task management component in Synology Download Station before 3.8.16-3566 allows remote authenticated users to execute arbitrary code via unspecified vectors.	2021-06-18	6.5	CVE-2021-34809 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
synology -- media_server	Server-Side Request Forgery (SSRF) vulnerability in cgi component in Synology Media Server before 1.8.3-2881 allows remote attackers to access intranet resources via unspecified vectors.	2021-06-18	5	CVE-2021-34808 CONFIRM
theologeek -- manuskript	** DISPUTED ** Manuskript through 0.12.0 allows remote attackers to execute arbitrary code via a crafted settings.pickle file in a project file, because there is insecure deserialization via the pickle.load() function in settings.py. NOTE: the vendor's position is that the product is not intended for opening an untrusted project file.	2021-06-21	6.8	CVE-2021-35196 MISC MISC
tielabs -- jannah	The Jannah WordPress theme before 5.4.4 did not properly sanitize the options JSON parameter in its tie_get_user_weather AJAX action before outputting it back in the page, leading to a Reflected Cross-Site Scripting (XSS) vulnerability.	2021-06-21	4.3	CVE-2021-24364 CONFIRM
typesettercms -- typesetter	Cross Site Scriptiong vulnerability in Typesetter 5.1 via the !1) className and !2) Description fields in index.php/Admin/Classes,	2021-06-21	4.3	CVE-2020-19511

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
ui -- camera_g3_flex_firmware	An issue was discovered in UniFi Protect G3 FLEX Camera Version UVC.v4.30.0.67.Attacker could send a huge amount of TCP SYN packet to make web service's resource exhausted. Then the web server is denial-of-service.	2021-06-18	5	CVE-2021-33820 MISC MISC MISC
ui -- camera_g3_flex_firmware	An issue was discovered in UniFi Protect G3 FLEX Camera Version UVC.v4.30.0.67. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service.	2021-06-18	5	CVE-2021-33818 MISC MISC MISC
vanillaforums -- vanilla_forums	It was found in vanilla forums before 2.0.10 a cross-site scripting vulnerability where a filename could contain arbitrary code to execute on the client side.	2021-06-22	4.3	CVE-2010-4264 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vanillaforums -- vanilla_forums	It was found in vanilla forums before 2.0.10 a potential linkbait vulnerability in dispatcher.	2021-06-22	5.8	CVE-2010-4266 MISC
vfsjfilechooser2_project -- vfsjfilechooser2	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in Vfsjfilechooser2 version 0.2.9 and below which occurs when the application attempts to validate crafted URIs.	2021-06-21	5	CVE-2021-29061 MISC MISC MISC MISC MISC
vmware -- tools	VMware Tools for Windows (11.x.y prior to 11.3.0) contains a denial-of-service vulnerability in the VM3DMP driver. A malicious actor with local user privileges in the Windows guest operating system, where VMware Tools is installed, can trigger a PANIC in the VM3DMP driver leading to a denial-of-service condition in the Windows guest operating system.	2021-06-18	4.9	CVE-2021-21997 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
white_shark_systems_project -- white_shark_systems	White Shark System (WSS) 1.3.2 has a SQL injection vulnerability. The vulnerability stems from the log_edit.php files failing to filter the csa_to_user parameter, remote attackers can exploit the vulnerability to obtain database sensitive information.	2021-06-21	5	CVE-2020-20469 MISC
white_shark_systems_project -- white_shark_systems	White Shark System (WSS) 1.3.2 is vulnerable to sensitive information disclosure via default_task_add.php, remote attackers can exploit the vulnerability to create a task.	2021-06-21	6.4	CVE-2020-20467 MISC
white_shark_systems_project -- white_shark_systems	White Shark System (WSS) 1.3.2 is vulnerable to CSRF. Attackers can use the user_edit_password.php file to modify the user password.	2021-06-21	4.3	CVE-2020-20468 MISC
white_shark_systems_project -- white_shark_systems	White Shark System (WSS) 1.3.2 has web site physical path leakage vulnerability.	2021-06-21	5	CVE-2020-20470 MISC
white_shark_systems_project -- white_shark_systems	White Shark System (WSS) 1.3.2 has a sensitive information disclosure vulnerability. The	2021-06-21	5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	if_get_addbook.php file does not have an authentication operation. Remote attackers can obtain username information for all users of the current site.			20472 MISC
white_shark_systems_project -- white_shark_systems	White Shark System (WSS) 1.3.2 has a SQL injection vulnerability. The vulnerability stems from the default_task_edituser.php files failing to filter the csa_to_user parameter. Remote attackers can exploit the vulnerability to obtain database sensitive information.	2021-06-21	5	CVE-2020-20474 MISC
white_shark_systems_project -- white_shark_systems	White Shark System (WSS) 1.3.2 has a SQL injection vulnerability. The vulnerability stems from the control_task.php, control_project.php, default_user.php files failing to filter the sort parameter. Remote attackers can exploit the vulnerability to obtain database sensitive information.	2021-06-21	5	CVE-2020-20473 MISC
wuzhicms -- wuzhicms	Cross Site Scripting (XSS) in Wuzhi CMS v4.1.0 allows remote attackers to execute arbitrary code via the "Title" parameter in the component "/coreframe/app/guestbook/myissue.php".	2021-06-22	4.3	CVE-2020-18654 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zettlr -- zettlr	No filtering of cross-site scripting (XSS) payloads in the markdown-editor in Zettlr 1.8.7 allows attackers to perform remote code execution via a crafted file.	2021-06-18	4.3	CVE-2021-26835 MISC MISC
zziplib_project -- zziplib	Infinite Loop in zziplib v0.13.69 allows remote attackers to cause a denial of service via the return value "zzip_file_read" in the function "unzzip_cat_file".	2021-06-18	4.3	CVE-2020-18442 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
admincolumns -- admin_columns	The Admin Columns Free WordPress plugin before 4.3 and Admin Columns Pro WordPress plugin before 5.5.1, rendered input on the posted pages with improper	2021-06-21	3.5	CVE-2021-24366

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	input validation on the value passed into the field 'Label' parameter, by taking this as an advantage an authenticated attacker can supply a crafted arbitrary script and execute it.			CONFIRM MISC
autoptimize -- autoptimize	The Autoptimize WordPress plugin before 2.7.8 does not check for malicious files such as .html in the archive uploaded via the 'Import Settings' feature. As a result, it is possible for a high privilege user to upload a malicious file containing JavaScript code inside an archive which will execute when a victim visits index.html inside the plugin directory.	2021-06-21	3.5	CVE-2021-24378 CONFIRM
ayecode -- getpaid	In the GetPaid WordPress plugin before 2.3.4, users with the contributor role and above can create a new Payment Form, however the Label and Help Text input fields were not getting sanitized properly. So it was possible to inject malicious content such as img tags, leading to a Stored Cross-Site Scripting issue which is triggered when the form will be edited, for example when an admin reviews it and could lead to privilege escalation.	2021-06-21	3.5	CVE-2021-24369 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
checksec -- canopy	CheckSec Canopy before 3.5.2 allows XSS attacks against the login page via the LOGIN_PAGE_DISCLAIMER parameter.	2021-06-18	3.5	CVE-2021-34815 MISC MISC MISC MISC
codecabin -- wp_google_maps	The WP Google Maps WordPress plugin before 8.1.12 did not sanitise, validate of escape the Map Name when output in the Map List of the admin dashboard, leading to an authenticated Stored Cross-Site Scripting issue	2021-06-21	3.5	CVE-2021-24383 CONFIRM MISC
get-simple -- getsimplecms	Cross Site Scripting vulnerability in GetSimpleCMS 3.4.0a in admin/snippets.php via (1) Add Snippet and (2) Save snippets.	2021-06-23	3.5	CVE-2020-20391 MISC
get-simple -- getsimplecms	Cross Site Scripting vulnerability in GetSimpleCMS 3.3.16 in admin/upload.php by adding comments or jpg and other file header information to the content of xla, pages, and gzip files,	2021-06-23	3.5	CVE-2021-28977 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
get-simple -- getsimplecms	Cross Site Scripting (XSS) vulnerability in GetSimpleCMS 3.4.0a in admin/edit.php.	2021-06-23	3.5	CVE-2020-20389 MISC
google -- android	In onStart of ContactsDumpActivity.java, there is possible access to contacts due to a tapjacking/overlay attack. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174045870	2021-06-22	1.9	CVE-2021-0569 MISC
google -- android	In sspRequestCallback of BondStateMachine.java, there is a possible leak of Bluetooth MAC addresses due to log information disclosure. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-183961896	2021-06-22	2.1	CVE-2021-0549 MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
google -- android	In doNotification of AccountManagerService.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-177931355	2021-06-22	2.1	CVE-2021-0572 MISC
google -- android	In accessAudioHalPidscpp of TimeCheck.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-175894436	2021-06-22	2.1	CVE-2021-0566 MISC
google -- android	In ih264e_fmt_conv_422i_to_420sp of ih264e_fmt_conv.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	2021-06-22	2.1	CVE-2021-0563 MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	exploitation.Product: AndroidVersions: Android-11Android ID: A-172908358			
google -- android	In RasterIntraUpdate of motion_est.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176084648	2021-06-22	2.1	CVE-2021-0562 MISC
google -- android	In append_to_verify_fifo_interleaved_ of stream_encoder.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174302683	2021-06-22	2.1	CVE-2021-0561 MISC
google -- android	In getBlockSum of fastcodemb.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional	2021-06-22	2.1	CVE-2021-0556 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172716941			
google -- android	In isBackupServiceActive of BackupManagerService.java, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-158482162	2021-06-22	2.1	CVE-2021-0554 MISC
google -- android	In getEndItemSliceAction of MediaOutputSlice.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-175124820	2021-06-22	2.1	CVE-2021-0552 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In updateNotification of BeamTransferManager.java, there is a missing permission check. This could lead to local information disclosure of paired Bluetooth addresses with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-168712890	2021-06-22	2.1	CVE-2021-0542 MISC
google -- android	In phNxpNciHal_ext_process_nfc_init_rsp of phNxpNciHal_ext.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the NFC server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169258455	2021-06-22	2.1	CVE-2021-0541 MISC
google -- android	In getAllPackages of PackageManagerService, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure of cross-user permissions with no additional execution privileges needed. User interaction is not	2021-06-21	2.1	CVE-2021-0521 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174661955			
google -- android	In avrc_pars_browse_rsp of avrc_pars_ct.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179162665	2021-06-21	3.3	CVE-2021-0504 MISC
icehrm -- icehrm	A stored cross site scripting (XSS) vulnerability was discovered in Ice Hrm 29.0.0.OS which allows attackers to execute arbitrary web scripts or HTML via a crafted file uploaded into the Document Management tab. The exploit is triggered when a user visits the upload location of the crafted file.	2021-06-22	3.5	CVE-2021-34243 MISC
jpress -- jpress	An issue was discovered in JPress v3.3.0 and below. There are XSS vulnerabilities in	2021-06-18	3.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the template module and tag management module. If you log in to the background by means of weak password, the storage XSS vulnerability can occur.			33347 MISC MISC
phpgurukul -- hospital_management_system_in_php	PHPGurukul Hospital Management System in PHP v4.0 has a Persistent Cross-Site Scripting vulnerability in \hms\admin\appointment-history.php. Remote registered users can exploit the vulnerability to obtain user cookie data.	2021-06-22	3.5	CVE-2020-22167 MISC
podsfoundation -- pods	The Pods â€“ Custom Content Types and Fields WordPress plugin before 2.7.27 was vulnerable to an Authenticated Stored Cross-Site Scripting (XSS) security vulnerability within the 'Menu Label' field parameter.	2021-06-21	3.5	CVE-2021-24339 MISC CONFIRM
podsfoundation -- pods	The Pods â€“ Custom Content Types and Fields WordPress plugin before 2.7.27 was vulnerable to an Authenticated Stored Cross-Site Scripting (XSS) security vulnerability within the 'Singular Label' field parameter.	2021-06-21	3.5	CVE-2021-24338 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wp_config_file_editor_project -- wp_config_file_editor	The WP Config File Editor WordPress plugin through 1.7.1 was affected by an Authenticated Stored Cross-Site Scripting (XSS) vulnerability.	2021-06-21	3.5	CVE-2021-24367 CONFIRM
znote -- znote	A cross-site scripting (XSS) vulnerability exists in Znote 0.5.2. An attacker can insert payloads, and the code execution will happen immediately on markdown view mode.	2021-06-18	3.5	CVE-2021-26834 MISC MISC