

Vulnerability Summary for the Week of August 2, 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 |
|---------------------------|--|------------|------------|--|
| bloofox -- bloofoxcms | bloofoxCMS 0.5.2.1 is infected with Unrestricted File Upload that allows attackers to upload malicious files (ex: php files). | 2021-06-16 | 7.5 | CVE-2020-35760 MISC |
| google -- android | In avrc_msg_cback of avrc_api.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution 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-177611958 | 2021-06-11 | 10 | CVE-2021-0474 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|---|------------|------------|---------------------------------------|
| google -- android | In memory management driver, 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 SoCAndroid ID: A-183464866 | 2021-06-11 | 7.2 | CVE-2021-0489 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-183461321 | 2021-06-11 | 7.2 | CVE-2021-0498 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-183461320 | 2021-06-11 | 7.2 | CVE-2021-0497 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-183467912 | 2021-06-11 | 7.2 | CVE-2021-0496 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|---|------------|------------|---------------------------------------|
| 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-183459083 | 2021-06-11 | 7.2 | CVE-2021-0495 MISC |
| google -- android | In memory management driver, 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 SoCAndroid ID: A-183461318 | 2021-06-11 | 7.2 | CVE-2021-0494 MISC |
| google -- android | In memory management driver, 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 SoCAndroid ID: A-183461317 | 2021-06-11 | 7.2 | CVE-2021-0493 MISC |
| google -- android | In memory management driver, 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 SoCAndroid ID: A-183459078 | 2021-06-11 | 7.2 | CVE-2021-0492 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|---|------------|------------|---------------------------------------|
| google -- android | In memory management driver, there is a possible escalation of privilege 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 SoCAndroid ID: A-183461315 | 2021-06-11 | 7.2 | CVE-2021-0491 MISC |
| google -- android | In memory management driver, 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 SoCAndroid ID: A-183464868 | 2021-06-11 | 7.2 | CVE-2021-0490 MISC |
| google -- android | In onCreate of CalendarDebugActivity.java, there is a possible way to export calendar data to the sdcard 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 not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174046397 | 2021-06-11 | 7.2 | CVE-2021-0487 MISC |
| google -- android | In onActivityResult of EditUserPhotoController.java, there is a possible access of unauthorized files due to an unexpected URI handler. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: | 2021-06-11 | 9.3 | CVE-2021-0481 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|--|------------|------------|--|
| | AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-172939189 | | | |
| google -- android | In getMinimalSize of PipBoundsAlgorithm.java, there is a possible bypass of restrictions on background processes 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-174302616 | 2021-06-11 | 7.2 | CVE-2021-0485 MISC |
| google -- android | In notifyScreenshotError of ScreenshotNotificationsController.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege 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-178189250 | 2021-06-11 | 7.2 | CVE-2021-0477 MISC |
| google -- android | An improper input validation vulnerability in sflacfd_get_frm() in libslacfdextractor library prior to SMR MAY-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process. | 2021-06-11 | 7.5 | CVE-2021-25387 MISC |
| google -- android | An improper input validation vulnerability in sdfffd_parse_chunk_FVER() in libsdffextractor library prior to SMR MAY-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process. | 2021-06-11 | 7.5 | CVE-2021- |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|---|------------|------------|-------------------------------------|
| | | | | 25386 MISC |
| google -- android | An improper input validation vulnerability in sdfffd_parse_chunk_PROP() in libsdffextractor library prior to SMR MAY-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process. | 2021-06-11 | 7.5 | CVE-2021-25385 MISC |
| google -- android | An improper input validation vulnerability in sdfffd_parse_chunk_PROP() with Sample Rate Chunk in libsdffextractor library prior to SMR MAY-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process. | 2021-06-11 | 7.5 | CVE-2021-25384 MISC |
| google -- android | An improper input validation vulnerability in scmn_mfal_read() in libsapeextractor library prior to SMR MAY-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process. | 2021-06-11 | 7.5 | CVE-2021-25383 MISC |
| google -- android | In on_l2cap_data_ind of btif_sock_l2cap.cc, there is possible memory corruption due to a use after free. 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-10Android ID: A-175686168 | 2021-06-11 | 8.3 | CVE-2021-0475 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|---|------------|------------|--|
| google -- android | In rw_t3t_process_error of rw_t3t.cc, there is a possible double free due to uninitialized data. This could lead to remote code execution over NFC 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-179687208 | 2021-06-11 | 8.3 | CVE-2021-0473 MISC |
| google -- android | An improper access control vulnerability in genericssoservice prior to SMR JUN-2021 Release 1 allows local attackers to execute protected activity with system privilege via untrusted applications. | 2021-06-11 | 7.2 | CVE-2021-25412 MISC |

Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|--------------------------------|--|------------|------------|---|
| bestwebsoft -- visitors_online | The Visitors WordPress plugin through 0.3 is affected by an Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability. The plugin would display the user's user agent string | 2021-06-14 | 4.3 | CVE-2021-24350 CONFIRM |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|--|------------|------------|--|
| | without validation or encoding within the WordPress admin panel. | | | |
| bloofox -- bloofoxcms | bloofoxCMS 0.5.2.1 is infected with Path traversal in the 'fileurl' parameter that allows attackers to read local files. | 2021-06-16 | 4 | CVE-2020-35762 MISC |
| bloofox -- bloofoxcms | bloofoxCMS 0.5.2.1 is infected with a CSRF Attack that leads to an attacker editing any file content (Locally/Remotely). | 2021-06-16 | 4.3 | CVE-2020-35759 MISC |
| google -- android | In FindOrCreatePeer of btif_av.cc, 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-9 Android-10Android ID: A-169252501 | 2021-06-11 | 6.9 | CVE-2021-0476 MISC |
| google -- android | An improper input validation vulnerability in NPU firmware prior to SMR MAY-2021 | 2021-06-11 | 4.6 | CVE-2021- |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|---|------------|------------|--|
| | Release 1 allows arbitrary memory write and code execution. | | | 25396 MISC |
| google -- android | In BinderDiedCallback of MediaCodec.cpp, 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-11Android ID: A-173791720 | 2021-06-11 | 6.9 | CVE-2021-0482 MISC |
| google -- android | In startIpClient of ClientModeImpl.java, there is a possible identifier which could be used to track a device. This could lead to remote information disclosure to a proximal attacker, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-154114734 | 2021-06-11 | 5 | CVE-2021-0466 MISC |
| google -- android | Improper authorization in SDP SDK prior to SMR JUN-2021 Release 1 allows access to internal storage. | 2021-06-11 | 5 | CVE-2021-25417 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|--|------------|------------|--------------------------------|
| google -- android | In shouldLockKeyguard of LockTaskController.java, there is a possible way to exit App Pinning without a PIN 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-11 Android-9 Android-10Android ID: A-176801033 | 2021-06-11 | 4.6 | CVE-2021-0472 MISC |
| google -- android | Improper sanitization of incoming intent in Samsung Contacts prior to SMR JUN-2021 Release 1 allows local attackers to copy or overwrite arbitrary files with Samsung Contacts privilege. | 2021-06-11 | 4.6 | CVE-2021-25414 MISC |
| google -- android | A possible out of bounds write vulnerability in NPU driver prior to SMR JUN-2021 Release 1 allows arbitrary memory write. | 2021-06-11 | 4.6 | CVE-2021-25407 MISC MISC |
| google -- android | A possible buffer overflow vulnerability in NPU driver prior to SMR JUN-2021 Release 1 allows arbitrary memory write and code execution. | 2021-06-11 | 4.6 | CVE-2021-25408 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|---|------------|------------|--|
| google -- android | A use after free vulnerability via race condition in MFC charger driver prior to SMR MAY-2021 Release 1 allows arbitrary write given a radio privilege is compromised. | 2021-06-11 | 4.4 | CVE-2021-25394 MISC |
| google -- android | A race condition in MFC charger driver prior to SMR MAY-2021 Release 1 allows local attackers to bypass signature check given a radio privilege is compromised. | 2021-06-11 | 4.4 | CVE-2021-25395 MISC |
| google -- android | In createPendingIntent of SnoozeHelper.java, there is a possible broadcast intent containing a sensitive identifier. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-174493336 | 2021-06-11 | 4.3 | CVE-2021-0480 MISC |
| google -- chrome | Type confusion in V8 in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2021-06-15 | 6.8 | CVE-2021-30551 MISC MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|---|------------|------------|--|
| google -- chrome | Use after free in Extensions in Google Chrome prior to 91.0.4472.101 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. | 2021-06-15 | 6.8 | CVE-2021-30552 MISC MISC |
| google -- chrome | Use after free in Network service in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2021-06-15 | 6.8 | CVE-2021-30553 MISC MISC |
| google -- chrome | Use after free in Spell check in Google Chrome prior to 91.0.4472.101 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. | 2021-06-15 | 6.8 | CVE-2021-30549 MISC MISC |
| google -- chrome | Use after free in Loader in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2021-06-15 | 6.8 | CVE-2021-30548 MISC MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|------------|------------|---|
| google -- chrome | Out of bounds write in ANGLE in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. | 2021-06-15 | 6.8 | CVE-2021-30547 MISC MISC |
| kohsei-works -- yes/no_chart | The Yes/No Chart WordPress plugin before 1.0.12 did not sanitise its sid shortcode parameter before using it in a SQL statement, allowing medium privilege users (contributor+) to perform Blind SQL Injection attacks | 2021-06-14 | 4 | CVE-2021-24360 CONFIRM |
| phpcms -- phpcms | Directory Traversal vulnerability in phpCMS 9.1.13 via the q parameter to public_get_suggest_keyword. | 2021-06-16 | 5 | CVE-2020-22200 MISC |
| posimyth -- the_plus_addons_for_elementor | The Plus Addons for Elementor Page Builder WordPress plugin before 4.1.11 did not properly check that a user requesting a password reset was the legitimate user, allowing an attacker to send an arbitrary reset password email to a registered user on behalf of the WordPress site. Such issue could be chained with an open redirect (CVE-2021- | 2021-06-14 | 5 | CVE-2021-24359 MISC CONFIRM |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|--|---|------------|------------|-----------------------------------|
| | 24358) in version below 4.1.10, to include a crafted password reset link in the email, which would lead to an account takeover. | | | |
| posimyth -- the_plus_addons_for_elementor | The Plus Addons for Elementor Page Builder WordPress plugin before 4.1.10 did not validate a redirect parameter on a specifically crafted URL before redirecting the user to it, leading to an Open Redirect issue. | 2021-06-14 | 5.8 | CVE-2021-24358 MISC CONFIRM |
| samsung -- galaxy_watch_active_2_firmware | Improper authentication vulnerability in Tizen bluetooth-frwk prior to Firmware update JUN-2021 Release allows bluetooth attacker to take over the user's bluetooth device without user awareness. | 2021-06-11 | 5.8 | CVE-2021-25424 MISC |
| samsung -- health | Improper check vulnerability in Samsung Health prior to version 6.17 allows attacker to read internal cache data via exported component. | 2021-06-11 | 5 | CVE-2021-25425 MISC |
| samsung -- internet | Improper component protection vulnerability in Samsung Internet prior to version 14.0.1.62 allows untrusted applications to execute arbitrary activity in specific condition. | 2021-06-11 | 4.4 | CVE-2021-25418 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|--|---|------------|------------|------------------------|
| schneider-electric -- interactive_graphical_scada_system | A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to lack of proper validation of user-supplied data, when a malicious CGF file is imported to IGSS Definition. | 2021-06-11 | 6.8 | CVE-2021-22754 MISC |
| schneider-electric -- interactive_graphical_scada_system | A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21041 and prior that could result in loss of data or remote code execution due to missing length checks, when a malicious CGF file is imported to IGSS Definition. | 2021-06-11 | 6.8 | CVE-2021-22750 MISC |
| schneider-electric -- interactive_graphical_scada_system | A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or execution of arbitrary code due to lack of input validation, when a malicious CGF (Configuration Group File) file is imported to IGSS Definition. | 2021-06-11 | 6.8 | CVE-2021-22751 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|--|--|------------|------------|--|
| schneider-electric -- interactive_graphical_scada_system | A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to missing size checks, when a malicious WSP (Workspace) file is being parsed by IGSS Definition. | 2021-06-11 | 6.8 | CVE-2021-22752 MISC |
| schneider-electric -- interactive_graphical_scada_system | A CWE-125: Out-of-bounds read vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to missing length checks, when a malicious WSP file is being parsed by IGSS Definition. | 2021-06-11 | 6.8 | CVE-2021-22753 MISC |
| schneider-electric -- interactive_graphical_scada_system | A CWE-125: Out-of-bounds read vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or remote code execution due to lack of sanity checks on user-supplied input data, when a malicious CGF file is imported to IGSS Definition. | 2021-06-11 | 6.8 | CVE-2021-22757 MISC |
| schneider-electric -- interactive_graphical_scada_system | A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could | 2021-06-11 | 6.8 | CVE-2021- |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|--|------------|------------|--|
| | result in disclosure of information or remote code execution due to lack of sanity checks on user-supplied data, when a malicious CGF file is imported to IGSS Definition. | | | 22755 MISC |
| schneider-electric -- interactive_graphical_scada_system | A CWE-125: Out-of-bounds read vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or remote code execution due to lack of user-supplied data validation, when a malicious CGF file is imported to IGSS Definition. | 2021-06-11 | 6.8 | CVE-2021-22756 MISC |
| schneider-electric -- interactive_graphical_scada_system | A CWE-824: Access of uninitialized pointer vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to lack validation of user-supplied input data, when a malicious CGF file is imported to IGSS Definition. | 2021-06-11 | 6.8 | CVE-2021-22758 MISC |
| schneider-electric -- interactive_graphical_scada_system | A CWE-763: Release of invalid pointer or reference vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to missing checks of user- | 2021-06-11 | 6.8 | CVE-2021-22760 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|--|--|------------|------------|--|
| | supplied input data, when a malicious CGF file is imported to IGSS Definition. | | | |
| schneider-electric -- interactive_graphical_scada_system | A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or remote code e+F15xecution due to missing length check on user supplied data, when a malicious CGF file is imported to IGSS Definition. | 2021-06-11 | 6.8 | CVE-2021-22761 MISC |
| schneider-electric -- interactive_graphical_scada_system | A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in remote code execution, when a malicious CGF or WSP file is being parsed by IGSS Definition. | 2021-06-11 | 6.8 | CVE-2021-22762 MISC |
| schneider-electric -- interactive_graphical_scada_system | A CWE-416: Use after free vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to use of unchecked input data, when a malicious CGF file is imported to IGSS Definition. | 2021-06-11 | 6.8 | CVE-2021-22759 MISC |

Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|--|------------|------------|--|
| bloofox -- bloofoxcms | bloofoxCMS 0.5.2.1 is infected with XSS that allows remote attackers to execute arbitrary JS/HTML Code. | 2021-06-16 | 3.5 | CVE-2020-35761 MISC |
| canonical -- ubuntu_linux | It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the xorg-hwe-18.04 package apport hooks, it could expose private data to other local users. | 2021-06-12 | 2.1 | CVE-2021-32555 MISC |
| canonical -- ubuntu_linux | It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the xorg package apport hooks, it could expose private data to other local users. | 2021-06-12 | 2.1 | CVE-2021-32554 MISC |
| canonical -- ubuntu_linux | It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-17 package apport hooks, it could expose private data to other local users. | 2021-06-12 | 2.1 | CVE-2021-32553 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|--|------------|------------|--|
| canonical -- ubuntu_linux | It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-16 package apport hooks, it could expose private data to other local users. | 2021-06-12 | 2.1 | CVE-2021-32552 MISC |
| canonical -- ubuntu_linux | It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-15 package apport hooks, it could expose private data to other local users. | 2021-06-12 | 2.1 | CVE-2021-32551 MISC |
| canonical -- ubuntu_linux | It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-14 package apport hooks, it could expose private data to other local users. | 2021-06-12 | 2.1 | CVE-2021-32550 MISC |
| canonical -- ubuntu_linux | It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-13 package apport hooks, it could expose private data to other local users. | 2021-06-12 | 2.1 | CVE-2021-32549 MISC |
| canonical -- ubuntu_linux | It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-8 package apport hooks, it could expose private data to other local users. | 2021-06-12 | 2.1 | CVE-2021-32548 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|---|------------|------------|--|
| canonical -- ubuntu_linux | It was discovered that read_file() in apport/hookutils.py would follow symbolic links or open FIFOs. When this function is used by the openjdk-lts package apport hooks, it could expose private data to other local users. | 2021-06-12 | 2.1 | CVE-2021-32547 MISC |
| fooplugins -- foogallery | In the Best Image Gallery & Responsive Photo Gallery â€™ FooGallery WordPress plugin before 2.0.35, the Custom CSS field of each gallery is not properly sanitised or validated before being being output in the page where the gallery is embed, leading to a stored Cross-Site Scripting issue. | 2021-06-14 | 3.5 | CVE-2021-24357 CONFIRM |
| google -- android | Improper caller check vulnerability in Knox Core prior to SMR MAY-2021 Release 1 allows attackers to install arbitrary app. | 2021-06-11 | 3.6 | CVE-2021-25388 MISC MISC |
| google -- android | Improper running task check in S Secure prior to SMR MAY-2021 Release 1 allows attackers to use locked app without authentication. | 2021-06-11 | 3.6 | CVE-2021-25389 MISC |
| google -- android | Assuming EL1 is compromised, an improper address validation in RKP prior to SMR JUN-2021 Release 1 | 2021-06-11 | 2.1 | CVE-2021- |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|--|------------|------------|--------------------------------|
| | allows local attackers to create executable kernel page outside code area. | | | 25416 MISC |
| google -- android | Assuming EL1 is compromised, an improper address validation in RKP prior to SMR JUN-2021 Release 1 allows local attackers to remap EL2 memory as writable. | 2021-06-11 | 2.1 | CVE-2021-25415 MISC |
| google -- android | Improper sanitization of incoming intent in Samsung Contacts prior to SMR JUN-2021 Release 1 allows local attackers to get permissions to access arbitrary data with Samsung Contacts privilege. | 2021-06-11 | 2.1 | CVE-2021-25413 MISC |
| google -- android | Improper sanitization of incoming intent in SecSettings prior to SMR MAY-2021 Release 1 allows local attackers to get permissions to access system uid data. | 2021-06-11 | 2.1 | CVE-2021-25393 MISC MISC |
| google -- android | Improper access control of a component in CallBGProvider prior to SMR JUN-2021 Release 1 allows local attackers to access arbitrary files with an escalated privilege. | 2021-06-11 | 3.6 | CVE-2021-25410 MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|--|------------|------------|--|
| google -- android | In /proc/net of the kernel filesystem, there is a possible information leak due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-9496886 | 2021-06-11 | 2.1 | CVE-2019-9475 MISC |
| google -- android | In readVector of IMediaPlayer.cpp, there is a possible read of uninitialized heap data 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-9 Android-10 Android-11 Android-8.1Android ID: A-173720767 | 2021-06-11 | 2.1 | CVE-2021-0484 MISC |
| google -- android | Intent redirection vulnerability in Secure Folder prior to SMR MAY-2021 Release 1 allows attackers to execute privileged action. | 2021-06-11 | 2.1 | CVE-2021-25391 MISC MISC |
| google -- android | Improper protection of backup path configuration in Samsung Dex prior to SMR MAY-2021 Release 1 allows local attackers to get sensitive information via changing the path. | 2021-06-11 | 2.1 | CVE-2021-25392 MISC MISC |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---------------------------|--|------------|------------|--|
| google -- android | An improper access control vulnerability in TelephonyUI prior to SMR MAY-2021 Release 1 allows local attackers to write arbitrary files of telephony process via untrusted applications. | 2021-06-11 | 2.1 | CVE-2021-25397 MISC MISC |
| google -- android | Improper address validation vulnerability in RKP api prior to SMR JUN-2021 Release 1 allows root privileged local attackers to write read-only kernel memory. | 2021-06-11 | 2.1 | CVE-2021-25411 MISC |
| google -- android | Improper access in Notification setting prior to SMR JUN-2021 Release 1 allows physically proximate attackers to set arbitrary notification via physically configuring device. | 2021-06-11 | 2.1 | CVE-2021-25409 MISC |
| google -- android | Intent redirection vulnerability in PhotoTable prior to SMR MAY-2021 Release 1 allows attackers to execute privileged action. | 2021-06-11 | 1.9 | CVE-2021-25390 MISC MISC |
| samsung -- bixby_voice | Intent redirection vulnerability in Bixby Voice prior to version 3.1.12 allows attacker to access contacts. | 2021-06-11 | 2.1 | CVE-2021- |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|----------------------------------|---|------------|------------|------------------------|
| | | | | 25398 MISC |
| samsung -- galaxy_watch_3_plugin | Improper log management vulnerability in Galaxy Watch3 PlugIn prior to version 2.2.09.21033151 allows attacker with log permissions to leak Wi-Fi password connected to the user smartphone within log. | 2021-06-11 | 2.1 | CVE-2021-25421 MISC |
| samsung -- galaxy_watch_plugin | Improper log management vulnerability in Galaxy Watch PlugIn prior to version 2.2.05.21033151 allows attacker with log permissions to leak Wi-Fi password connected to the user smartphone within log. | 2021-06-11 | 2.1 | CVE-2021-25420 MISC |
| samsung -- gear_s | Information exposure vulnerability in Gear S Plugin prior to version 2.2.05.20122441 allows untrusted applications to access connected BT device information. | 2021-06-11 | 3.3 | CVE-2021-25406 MISC |
| samsung -- watch_active2_plugin | Improper log management vulnerability in Watch Active2 PlugIn prior to 2.2.08.21033151 version allows attacker with log permissions to leak Wi-Fi password connected to the user smartphone via log. | 2021-06-11 | 2.1 | CVE-2021-25423 MISC |
| samsung -- watch_active_plugin | Improper log management vulnerability in Watch Active PlugIn prior to version 2.2.07.21033151 allows attacker | 2021-06-11 | 2.1 | CVE-2021- |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|----------------------------------|--|------------------|-------------------|---|
| | with log permissions to leak Wi-Fi password connected to the user smartphone within log. | | | 25422 MISC |