SSA-770721: Multiple Vulnerabilities in SIMATIC RF160B before V2.2

Publication Date:	2024-03-12
Last Update:	2024-03-12
Current Version:	V1.0
CVSS v3.1 Base Score:	9.8

SUMMARY

SIMATIC RF160B contain multiple vulnerabilities of different types that could allow an attacker to execute arbitrary code within the context of a privileged process.

Siemens has released a new version for SIMATIC RF160B and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC RF160B (6GT2003-0FA00): All versions < V2.2 affected by all CVEs	Update to V2.2 or later version Contact customer support to receive patch and update information.

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

SIMATIC RF160B is a mobile reader that complements the SIMATIC RF200/300 (HF) and RF600 (UHF) RFID readers.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2017-14491

An attacker could cause a crash or potentially execute arbitrary code by sending specially crafted DNS responses to the DNSmasq process. In order to exploit this vulnerability, an attacker must be able to trigger DNS requests from the device, and must be in a privileged position to inject malicious DNS responses.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2017-18509

An issue was discovered in net/ipv6/ip6mr.c in the Linux kernel before 4.11. By setting a specific socket option, an attacker can control a pointer in kernel land and cause an inet_csk_listen_stop general protection fault, or potentially execute arbitrary code under certain circumstances. The issue can be triggered as root (e.g., inside a default LXC container or with the CAP_NET_ADMIN capability) or after namespace unsharing. This occurs because sk_type and protocol are not checked in the appropriate part of the ip6_mroute_* functions. NOTE: this affects Linux distributions that use 4.9.x longterm kernels before 4.9.187.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-0338

In checkKeyIntent of AccountManagerService.java, there is a possible permission bypass. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-9Android ID: A-123700107

CVSS v3.1 Base Score	5.0
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-0417

In setNiNotification of GpsNetInitiatedHandler.java, there is a possible permissions bypass due to an empty mutable 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-8.1 Android-9Android ID: A-154319182

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2020-10768

A flaw was found in the Linux Kernel before 5.8-rc1 in the prctl() function, where it can be used to enable indirect branch speculation after it has been disabled. This call incorrectly reports it as being ‘force disabled’ when it is not and opens the system to Spectre v2 attacks. The highest threat from this vulnerability is to confidentiality.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-440: Expected Behavior Violation

Vulnerability CVE-2020-11301

Improper authentication of un-encrypted plaintext Wi-Fi frames in an encrypted network can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2020-14305

An out-of-bounds memory write flaw was found in how the Linux kernel's Voice Over IP H.323 connection tracking functionality handled connections on ipv6 port 1720. This flaw allows an unauthenticated remote user to crash the system, causing a denial of service. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2020-14381

A flaw was found in the Linux kernel's futex implementation. This flaw allows a local attacker to corrupt system memory or escalate their privileges when creating a futex on a filesystem that is about to be unmounted. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2020-15436

Use-after-free vulnerability in fs/block_dev.c in the Linux kernel before 5.8 allows local users to gain privileges or cause a denial of service by leveraging improper access to a certain error field.

CVSS v3.1 Base Score	6.7
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2020-24587

The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that all fragments of a frame are encrypted under the same key. An adversary can abuse this to decrypt selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP encryption key is periodically renewed.

CVSS v3.1 Base Score	2.6
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:U/RL:U/RC:C
CWE	CWE-326: Inadequate Encryption Strength

Vulnerability CVE-2020-25705

A flaw in ICMP packets in the Linux kernel was found to allow to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypass source port UDP randomization. Software that relies on UDP source port randomization are indirectly affected as well. Kernel versions before 5.10 may be vulnerable to this issue.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C
CWE	CWE-330: Use of Insufficiently Random Values

Vulnerability CVE-2020-26555

Bluetooth legacy BR/EDR PIN code pairing in Bluetooth Core Specification 1.0B through 5.2 may permit an unauthenticated nearby device to spoof the BD_ADDR of the peer device to complete pairing without knowledge of the PIN.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-863: Incorrect Authorization

Vulnerability CVE-2020-26558

Bluetooth LE and BR/EDR secure pairing in Bluetooth Core Specification 2.1 through 5.2 may permit a nearby man-in-the-middle attacker to identify the Passkey used during pairing (in the Passkey authentication procedure) by reflection of the public key and the authentication evidence of the initiating device, potentially permitting this attacker to complete authenticated pairing with the responding device using the correct Passkey for the pairing session. The attack methodology determines the Passkey value one bit at a time.

CVSS v3.1 Base Score	4.2
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2020-29660

A locking inconsistency issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_io.c and drivers/tty/tty_jobctrl.c may allow a read-after-free attack against TIOCGSID, aka CID-c8bcd9c5be24.

CVSS v3.1 Base Score	4.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-667: Improper Locking

Vulnerability CVE-2020-29661

A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-667: Improper Locking

Vulnerability CVE-2021-0302

In PackageInstaller, there is a possible tapjacking attack due to an insecure default value. This could lead to local escalation of privilege and permissions with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10Android ID: A-155287782

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Vulnerability CVE-2021-0305

In PackageInstaller, there is a possible tapjacking attack due to an insecure default value. This could lead to local escalation of privilege and permissions with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10Android ID: A-154015447

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Vulnerability CVE-2021-0325

In ih264d_parse_pslice of ih264d_parse_pslice.c, 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 needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-174238784

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0326

In p2p_copy_client_info of p2p.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution if the target device is performing a Wi-Fi Direct search, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-172937525

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0327

In getContentProviderImpl of ActivityManagerService.java, there is a possible permission bypass due to non-restored binder identities. 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-172935267

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-269: Improper Privilege Management

Vulnerability CVE-2021-0328

In onBatchScanReports and deliverBatchScan of GattService.java, there is a possible way to retrieve Bluetooth scan results without permissions 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-10 Android-11 Android-8.1 Android-9Android ID: A-172670415

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2021-0329

In several native functions called by AdvertiseManager.java, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the Bluetooth server with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-171400004

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0330

In add_user_ce and remove_user_ce of storaged.cpp, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in storaged with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11Android ID: A-170732441

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0331

In onCreate of NotificationAccessConfirmationActivity.java, there is a possible overlay attack due to an insecure default value. This could lead to local escalation of privilege and notification access with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-170731783

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Vulnerability CVE-2021-0333

In onCreate of BluetoothPermissionActivity.java, there is a possible permissions bypass due to a tapjacking overlay that obscures the phonebook permissions dialog when a Bluetooth device is connecting. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-168504491

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Vulnerability CVE-2021-0334

In onTargetSelected of ResolverActivity.java, there is a possible settings bypass allowing an app to become the default handler for arbitrary domains. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-163358811

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2021-0336

In onReceive of BluetoothPermissionRequest.java, there is a possible permissions bypass due to a mutable PendingIntent. This could lead to local escalation of privilege that bypasses a permission check, with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-158219161

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2021-0337

In moveInMediaStore of FileSystemProvider.java, there is a possible file exposure due to stale metadata. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-157474195

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-312: Cleartext Storage of Sensitive Information

Vulnerability CVE-2021-0339

In loadAnimation of WindowContainer.java, there is a possible way to keep displaying a malicious app while a target app is brought to the foreground. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-8.1 Android-9Android ID: A-145728687

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

Vulnerability CVE-2021-0341

In verifyHostName of OkHostnameVerifier.java, there is a possible way to accept a certificate for the wrong domain due to improperly used crypto. This could lead to remote information disclosure 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-171980069

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

Vulnerability CVE-2021-0390

In various methods of WifiNetworkSuggestionsManager.java, there is a possible modification of suggested networks due to a missing permission check. This could lead to local escalation of privilege by a background user on the same device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174749461

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2021-0391

In onCreate() of ChooseTypeAndAccountActivity.java, there is a possible way to learn the existence of an account, without permissions, 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-11 Android-8.1 Android-9 Android-10Android ID: A-172841550

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Vulnerability CVE-2021-0392

In main of main.cpp, there is a possible memory corruption due to a double free. 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-9Android ID: A-175124730

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-415: Double Free

Vulnerability CVE-2021-0393

In Scanner::LiteralBuffer::NewCapacity of scanner.cc, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution if an attacker can supply a malicious PAC file, 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-168041375

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2021-0394

In android_os_Parcel_readString8 of android_os_Parcel.cpp, there is a possible out of bounds read 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-11 Android-8.1 Android-9 Android-10Android ID: A-172655291

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-0396

In Builtins::Generate_ArgumentsAdaptorTrampoline of builtins-arm.cc and related files, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution in an unprivileged process 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-160610106

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0397

In sdp_copy_raw_data of sdp_discovery.cc, there is a possible system compromise due to a double free. 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-174052148

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-415: Double Free

Vulnerability CVE-2021-0399

In qtaguid_untag of xt_qtaguid.c, 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 kernelAndroid ID: A-176919394References: Upstream kernel

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0400

In injectBestLocation and handleUpdateLocation of GnssLocationProvider.java, there is a possible incorrect reporting of location data to emergency services due to improper input validation. This could lead to incorrect reporting of location data to emergency services with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11Android ID: A-177561690

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-0429

In pollOnce of ALooper.cpp, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-175074139

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0431

In avrc_msg_cback of avrc_api.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a paired device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174149901

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-0433

In onCreate of DeviceChooserActivity.java, there is a possible way to bypass user consent when pairing a Bluetooth device due to a tapjacking/overlay attack. This could lead to local escalation of privilege and pairing malicious devices with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-171221090

CVSS v3.1 Base Score	8.0
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Vulnerability CVE-2021-0434

In onReceive of BluetoothPermissionRequest.java, there is a possible phishing attack allowing a malicious Bluetooth device to acquire permissions based on insufficient information presented to the user in the consent dialog. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-167403112

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2021-0435

In avrc_proc_vendor_command of avrc_api.cc, there is a possible leak of heap data due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174150451

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-665: Improper Initialization

Vulnerability CVE-2021-0436

In CryptoPlugin::decrypt of CryptoPlugin.cpp, there is a possible out of bounds read due to integer overflow. This could lead to local information disclosure 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-176496160

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2021-0437

In setPlayPolicy of DrmPlugin.cpp, there is a possible double free. This could lead to local escalation of privilege in a privileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-176168330

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-415: Double Free

Vulnerability CVE-2021-0438

In several functions of InputDispatcher.cpp, WindowManagerService.java, and related files, there is a possible tapjacking attack due to an incorrect FLAG_OBSCURED value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10Android ID: A-152064592

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Vulnerability CVE-2021-0443

In several functions of ScreenshotHelper.java and related files, there is a possible incorrectly saved screenshot due to a race condition. This could lead to local information disclosure across user profiles with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-170474245

CVSS v3.1 Base Score	4.7
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2021-0444

In onActivityResult of QuickContactActivity.java, there is an unnecessary return of an intent. This could lead to local information disclosure of contact data with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-178825358

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2021-0471

In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds read due to an integer overflow. 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-176444786

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2021-0473

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

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-908: Use of Uninitialized Resource

Vulnerability CVE-2021-0474

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

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0476

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

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2021-0478

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

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-755: Improper Handling of Exceptional Conditions

Vulnerability CVE-2021-0480

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

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2021-0481

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: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-172939189

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-0484

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

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-909: Missing Initialization of Resource

Vulnerability CVE-2021-0506

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 needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-181962311

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Vulnerability CVE-2021-0507

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

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0508

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

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0509

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

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0510

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

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2021-0511

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 exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11Android ID: A-178055795

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-0512

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

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0513

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

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2021-0514

In several functions of the V8 library, there is a possible use after free due to a race condition. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-9 Android-11 Android-8.1Android ID: A-162604069

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2021-0515

In Factory::CreateStrictFunctionMap of factory.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution in an unprivileged process 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-167389063

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0516

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

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0519

In BITSTREAM_FLUSH of ih264e_bitstream.h, there is a possible out of bounds write 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 exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-176533109

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0520

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

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0521

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 needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174661955

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2021-0522

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

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0584

In verifyBufferObject of Parcel.cpp, there is a possible out of bounds read due to an improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-179289794

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-0585

In beginWrite and beginRead of MessageQueueBase.h, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-184963385

CVSS v3.1 Base Score	6.7
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0586

In onCreate of DevicePickerFragment.java, there is a possible way to trick the user to select an unwanted bluetooth device due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-182584940

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Vulnerability CVE-2021-0587

In StreamOut::prepareForWriting of StreamOut.cpp, 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-8.1 Android-9 Android-10 Android-11Android ID: A-185259758

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0588

In processInboundMessage of MceStateMachine.java, there is a possible SMS disclosure due to 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-8.1 Android-9Android ID: A-177238342

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-668: Exposure of Resource to Wrong Sphere

Vulnerability CVE-2021-0589

In BTM_TryAllocateSCN of btm_scn.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-180939982

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0591

In sendReplyIntentToReceiver of BluetoothPermissionActivity.java, there is a possible way to invoke privileged broadcast receivers due to a confused deputy. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-179386960

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-610: Externally Controlled Reference to a Resource in Another Sphere

Vulnerability CVE-2021-0593

In sendDevicePickedIntent of DevicePickerFragment.java, there is a possible way to invoke a privileged broadcast receiver due to a confused deputy. 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-179386068

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-610: Externally Controlled Reference to a Resource in Another Sphere

Vulnerability CVE-2021-0594

In onCreate of ConfirmConnectActivity, there is a possible remote bypass of user consent due to improper input validation. This could lead to remote (proximal, NFC) escalation of privilege allowing an attacker to deceive a user into allowing a Bluetooth connection with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-176445224

CVSS v3.1 Base Score	8.0
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

Vulnerability CVE-2021-0596

In phNciNfc_RecvMfResp of phNxpExtns_MifareStd.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over NFC 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-181346550

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-0597

In notifyProfileAdded and notifyProfileRemoved of SipService.java, there is a possible way to retrieve SIP account names due to 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-8.1 Android-9 Android-10 Android-11Android ID: A-176496502

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2021-0598

In onCreate of ConfirmConnectActivity.java, there is a possible pairing of untrusted Bluetooth devices 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-11 Android-8.1 Android-9 Android-10Android ID: A-180422108

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Vulnerability CVE-2021-0599

In scheduleTimeoutLocked of NotificationRecord.java, there is a possible disclosure of a sensitive identifier via broadcasted intent due to a confused deputy. 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-175614289

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-610: Externally Controlled Reference to a Resource in Another Sphere

Vulnerability CVE-2021-0600

In onCreate of DeviceAdminAdd.java, there is a possible way to mislead a user to activate a device admin app due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-179042963

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-0601

In encodeFrames of avc_enc_fuzzer.cpp, there is a possible out of bounds write due to a double free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-180643802

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-415: Double Free

Vulnerability CVE-2021-0604

In generateFileInfo of BluetoothOppSendFileInfo.java, there is a possible way to share private files over Bluetooth due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-179910660

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2021-0640

In noteAtomLogged of StatsdStats.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-187957589

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0641

In getAvailableSubscriptionInfoList of SubscriptionController.java, there is a possible disclosure of unique identifiers due to 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-8.1 Android-9 Android-10 Android-11Android ID: A-185235454

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2021-0642

In onResume of VoicemailSettingsFragment.java, there is a possible way to retrieve a trackable identifier without permissions due to a missing permission check. 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-185126149

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2021-0646

In sqlite3_str_vappendf of sqlite3.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege if the user can also inject a printf into a privileged process's SQL 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-153352319

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0650

In WT_InterpolateNoLoop of eas_wtengine.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-190286685

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-0651

In loadLabel of PackageItemInfo.java, there is a possible way to DoS a device by having a long label in an app due to incorrect input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-9 Android-10Android ID: A-67013844

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-0652

In VectorDrawable::VectorDrawable of VectorDrawable.java, there is a possible way to introduce a memory corruption due to sharing of not thread-safe objects. 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-185178568

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2021-0653

In enqueueNotification of NetworkPolicyManagerService.java, there is a possible way to retrieve a trackable identifier due to 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-10 Android-11 Android-9Android ID: A-177931370

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2021-0682

In sendAccessibilityEvent of NotificationManagerService.java, there is a possible disclosure of notification data due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-159624555

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2021-0683

In runTraceIpcStop of ActivityManagerShellCommand.java, there is a possible deletion of system files 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-11 Android-8.1 Android-9 Android-10Android ID: A-185398942

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2021-0684

In TouchInputMapper::sync of TouchInputMapper.cpp, 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-10 Android-11 Android-8.1 Android-9Android ID: A-179839665

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0687

In ellipsize of Layout.java, there is a possible ANR due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-188913943

CVSS v3.1 Base Score	5.0
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-834: Excessive Iteration

Vulnerability CVE-2021-0688

In lockNow of PhoneWindowManager.java, there is a possible lock screen bypass due to a race condition. 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-161149543

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2021-0689

In RGB_to_BGR1_portable of SkSwizzler_opts.h, there is a possible out of bounds read 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-10 Android-11 Android-8.1 Android-9Android ID: A-190188264

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-0690

In ih264d_mark_err_slice_skip of ih264d_parse_pslice.c, there is a possible out of bounds write 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-9 Android-10 Android-11 Android-8.1Android ID: A-182152757

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0692

In sendBroadcastToInstaller of FirstScreenBroadcast.java, there is a possible activity launch due to an unsafe PendingIntent. 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-179289753

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2021-0695

In get_sock_stat of xt_qtaguid.c, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-184018316References: Upstream kernel

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0704

In createNoCredentialsPermissionNotification and related functions of AccountManagerService.java, there is a possible way to retrieve accounts from the device without permissions 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-10 Android-11 Android-9Android ID: A-179338675

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-281: Improper Preservation of Permissions

Vulnerability CVE-2021-0706

In startListening of PluginManagerImpl.java, there is a possible way to disable arbitrary app components due to a missing permission check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-193444889

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2021-0708

In runDumpHeap of ActivityManagerShellCommand.java, there is a possible deletion of system files 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-9 Android-10 Android-11 Android-8.1Android ID: A-183262161

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-610: Externally Controlled Reference to a Resource in Another Sphere

Vulnerability CVE-2021-0870

In RW_SetActivatedTagType of rw_main.cc, there is possible memory corruption due to a race condition. This could lead to remote code execution 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-192472262

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2021-0919

In getService of IServiceManager.cpp, there is a possible unhandled exception due to an integer overflow. This could lead to local denial of service making the lockscreen unusable with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-197336441

CVSS v3.1 Base Score	5.0
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2021-0920

In unix_scm_to_skb of af_unix.c, there is a possible use after free bug 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 kernelAndroid ID: A-196926917References: Upstream kernel

CVSS v3.1 Base Score	6.4
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0926

In onCreate of NfcImportVCardActivity.java, there is a possible way to add a contact without user's 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 exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-191053931

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2021-0928

In createFromParcel of OutputConfiguration.java, there is a possible parcel serialization/deserialization mismatch 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 exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-188675581

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-755: Improper Handling of Exceptional Conditions

Vulnerability CVE-2021-0929

In ion_dma_buf_end_cpu_access and related functions of ion.c, there is a possible way to corrupt memory 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 kernelAndroid ID: A-187527909References: Upstream kernel

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-0930

In phNxpNciHal_process_ext_rsp of phNxpNciHal_ext.cc, there is a possible out of bounds write due to a missing bounds check. 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-10 Android-11 Android-12 Android-9Android ID: A-181660091

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0931

In getAlias of BluetoothDevice.java, there is a possible way to create misleading permission dialogs due to missing data filtering. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-180747689

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2021-0933

In onCreate of CompanionDeviceActivity.java or DeviceChooserActivity.java, there is a possible way for HTML tags to interfere with a consent dialog due to improper input validation. This could lead to remote escalation of privilege, confusing the user into accepting pairing of a malicious Bluetooth device, with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-172251622

CVSS v3.1 Base Score	8.0
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-116: Improper Encoding or Escaping of Output

Vulnerability CVE-2021-0952

In doCropPhoto of PhotoSelectionHandler.java, there is a possible permission bypass due to a confused deputy. This could lead to local information disclosure of user's contacts with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-195748381

CVSS v3.1 Base Score	5.0
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2021-0953

In setOnClickActivityIntent of SearchWidgetProvider.java, there is a possible way to access contacts and history bookmarks without permission 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-12 Android-9Android ID: A-184046278

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-281: Improper Preservation of Permissions

Vulnerability CVE-2021-0961

In quota_proc_write of xt_quota2.c, there is a possible way to read kernel memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-196046570References: Upstream kernel

CVSS v3.1 Base Score	4.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-909: Missing Initialization of Resource

Vulnerability CVE-2021-0963

In onCreate of KeyChainActivity.java, there is a possible way to use an app certificate stored in keychain due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-199754277

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Vulnerability CVE-2021-0964

In C2SoftMP3::process() of C2SoftMp3Dec.cpp, there is a possible out of bounds write 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-10 Android-11 Android-12 Android-9Android ID: A-193363621

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-681: Incorrect Conversion between Numeric Types

Vulnerability CVE-2021-0965

In AndroidManifest.xml of Settings, there is a possible pairing of a Bluetooth device without user's 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 exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-194300867

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

Vulnerability CVE-2021-0967

In vorbis_book_decodev_set of codebook.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-199065614

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-0968

In osi_malloc and osi_calloc of allocator.cc, 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 not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-197868577

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2021-0970

In createFromParcel of GpsNavigationMessage.java, there is a possible Parcel serialization/deserialization mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-196970023

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-502: Deserialization of Untrusted Data

Vulnerability CVE-2021-1972

Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2021-1976

A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-29647

An issue was discovered in the Linux kernel before 5.11.11. qrtr_recvmsg in net/qrtr/qrtr.c allows attackers to obtain sensitive information from kernel memory because of a partially uninitialized data structure, aka CID-50535249f624.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-909: Missing Initialization of Resource

Vulnerability CVE-2021-33909

fs/seq_file.c in the Linux kernel 3.16 through 5.13.x before 5.13.4 does not properly restrict seq buffer allocations, leading to an integer overflow, an Out-of-bounds Write, and escalation to root by an unprivileged user, aka CID-8cae8cd89f05.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2021-38204

drivers/usb/host/max3421-hcd.c in the Linux kernel before 5.13.6 allows physically proximate attackers to cause a denial of service (use-after-free and panic) by removing a MAX-3421 USB device in certain situations.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-39621

In sendLegacyVoicemailNotification of LegacyModeSmsHandler.java, there is a possible permissions 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-12 Android-9Android ID: A-185126319

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2021-39623

In doRead of SimpleDecodingSource.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-194105348

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-39626

In onAttach of ConnectedDeviceDashboardFragment.java, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-194695497

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-610: Externally Controlled Reference to a Resource in Another Sphere

Vulnerability CVE-2021-39627

In sendLegacyVoicemailNotification of LegacyModeSmsHandler.java, there is a possible permissions 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-12 Android-9Android ID: A-185126549

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2021-39629

In phTmlNfc_Init and phTmlNfc_CleanUp of phTmlNfc.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-10 Android-11 Android-12 Android-9Android ID: A-197353344

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-39633

In gre_handle_offloads of ip_gre.c, there is a possible page fault due to an invalid memory access. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-150694665References: Upstream kernel

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2021-39634

In fs/eventpoll.c, there is a possible 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 kernelAndroid ID: A-204450605References: Upstream kernel

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2022-20127

In ce_t4t_data_cback of ce_t4t.cc, there is a possible out of bounds write due to a double free. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-221862119

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-415: Double Free

Vulnerability CVE-2022-20130

In transportDec_OutOfBandConfig of tpdec_lib.cpp, 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-10 Android-11 Android-12 Android-12LAndroid ID: A-224314979

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

Vulnerability CVE-2022-20227

In USB driver, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-216825460References: Upstream kernel

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-20229

In bta_hf_client_handle_cind_list_item of bta_hf_client_at.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-224536184

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-20355

In get of PacProxyService.java, there is a possible system service crash due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-219498290

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2022-20411

In avdt_msg_asmbl of avdt_msg.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-10 Android-11 Android-12 Android-12L Android-13Android ID: A-232023771

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-20421

In binder_inc_ref_for_node of binder.c, there is a possible way to corrupt memory 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 kernelAndroid ID: A-239630375References: Upstream kernel

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2022-20422

In emulation_proc_handler of armv8_deprecated.c, there is a possible way to corrupt memory 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 kernelAndroid ID: A-237540956References: Upstream kernel

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2022-20423

In rndis_set_response of rndis.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege if a malicious USB device is attached with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239842288References: Upstream kernel

CVSS v3.1 Base Score	4.6
CVSS Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-20462

In phNxpNciHal_write_unlocked 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 no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230356196

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-20466

In applyKeyguardFlags of NotificationShadeWindowControllerImpl.java, there is a possible way to observe the user's password on a secondary display due to an insecure default value. 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-12 Android-12L Android-13Android ID: A-179725730

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-1188: Initialization of a Resource with an Insecure Default

Vulnerability CVE-2022-20468

In BNEP_ConnectResp of bnep_api.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-228450451

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-20469

In avct_lcb_msg_asmbl of avct_lcb_act.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230867224

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-20472

In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239210579

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-20473

In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239267173

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-20476

In setEnabledSetting of PackageManager.java, there is a possible way to get the device into an infinite reboot loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-240936919

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability CVE-2022-20483

In several functions that parse avrc response in avrc_pars_ct.cc and related files, there are possible out of bounds reads due to integer overflows. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242459126

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-191: Integer Underflow (Wrap or Wraparound)

Vulnerability CVE-2022-20498

In fdt_path_offset_namelen of fdt_ro.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-246465319

CVSS v3.1 Base Score	4.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-20500

In loadFromXml of ShortcutPackage.java, there is a possible crash on boot due to an uncaught exception. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-246540168

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-755: Improper Handling of Exceptional Conditions

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2024-03-12):	Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.