Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Android OS – 4th March 2026

Document ID	SMA-Informative Cyber Alert
Document status	ISSUED
Authors	Marian Matache <marian.matache@smarttech247.com>
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	4th March 2026
Issue Date	4th March 2026

Informative Cyber Alerts are reports created by Smarttech247 designed to inform customers about medium and low severity vulnerabilities, IOCs from certain attacks/breaches, and other information that could help companies be aware and protect against any attack.
The content of this report should be regarded as simply informative as it usually addresses products that have an auto-update option available for patches. It will be the customer's decision if it is necessary to follow any recommendation or disregard them as they are not currently applicable in the environment.

Overview

Multiple vulnerabilities have been identified in the Google Android operating system, the most severe of which could enable remote code execution. Android is a mobile operating system developed by Google and used across smartphones, tablets, wearables, and other devices. Successful exploitation of the most critical vulnerabilities may allow an attacker to execute arbitrary code remotely. Depending on the privileges of the compromised component, the attacker could install applications, view/modify/delete data, or create new accounts with full administrative rights.

Technical Summary

2025-12-05 security patch level vulnerability details

Multiple vulnerabilities have been discovered in Google Android OS, the most severe of which could allow for remote code execution in the context of the affected component. Following the MITRE ATT&CK framework, exploitation of these vulnerabilities can be classified as follows:

Tactic: Execution (TA0002)
Technique: Exploitation for Client Execution (T1203)

Android and Google Service Mitigations

This section summarizes the mitigations provided by the Android security platform and service protections such as Google Play Protect. These capabilities reduce the likelihood that security vulnerabilities could be successfully exploited on Android. Exploitation for many issues is made more difficult by the ongoing enhancements introduced in recent Android platform releases. We encourage all users to update to the latest version of Android where possible.

The Android security team actively monitors for abuse through Google Play Protect and warns users about Potentially Harmful Applications. Google Play Protect is enabled by default on devices with Google Mobile Services and is particularly important for users who install apps from outside Google Play.

Google notifies Android partners of all issues at least one month prior to publishing the bulletin.

2026-03-01 security patch level vulnerability details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2026-03-01 patch level. Vulnerabilities are grouped under the component they affect. Issues are described in the tables below and include CVE ID, associated references, type of vulnerability, severity, and updated AOSP versions (where applicable). When

available, we link the public change that addressed the issue to the bug ID, like the AOSP change list. When multiple changes relate to a single bug, additional references are linked to numbers following the bug ID. Devices with Android 10 and later may receive security updates as well as Google Play system updates.

Framework

The most severe vulnerability in this section could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

The following CVEs have high severity and have not yet been documented or assigned a score:
CVE-2026-0047, CVE-2025-32313, CVE-2025-48544, CVE-2025-48567, CVE-2025-48568, CVE-2025-48574, CVE-2025-48577, CVE-2025-48578, CVE-2025-48579, CVE-2025-48582, CVE-2025-48605, CVE-2025-48619, CVE-2025-48634, CVE-2025-48635, CVE-2025-48645, CVE-2025-48646, CVE-2025-48654, CVE-2026-0007, CVE-2026-0008, CVE-2026-0010, CVE-2026-0011, CVE-2026-0013, CVE-2026-0020, CVE-2026-0023, CVE-2026-0026, CVE-2026-0034, CVE-2025-48630, CVE-2026-0012, CVE-2026-0025, CVE-2025-48644, CVE-2026-0014, CVE-2026-0015

System

The most severe vulnerability in this section could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.

CVE ID	Description	CVSS Score
CVE-2026-0006	In multiple locations, there is a possible out of bounds read and 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.	9.8
CVE-2025-48602	In exitKeyguardAndFinishSurfaceBehindRemoteAnimation of KeyguardViewMediator.java, there is a possible lockscreen bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4
CVE-2025-48641	In multiple functions of Nfc.h, 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.	7.0
CVE-2025-48650	In multiple locations, there is a possible information disclosure due to SQL injection. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4
CVE-2025-48653	In loadDataAndPostValue of multiple files, there is a possible way to obscure permission usage due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4
CVE-2026-0017	In onChange of BiometricService.java, there is a possible way to enable fingerprint unlock due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.7
CVE-2026-0021	In hasInteractAcrossUsersFullPermission of AppInfoBase.java, there is a possible cross-user permission bypass 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.	8.4
CVE-2026-0035	In createRequest of MediaProvider.java, there is a possible way for an app to gain read/write access to non-existing files due to a logic error in the code. This could lead to local escalation of	8.4

	privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	
CVE-2025-64783	DNG SDK versions 1.7.0 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8
CVE-2025-64784	DNG SDK versions 1.7.0 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could lead to memory exposure or application denial of service. An attacker could leverage this vulnerability to disclose sensitive memory information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.1
CVE-2025-64893	DNG SDK versions 1.7.0 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure or application denial of service. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.1
CVE-2025-48609	In multiple functions of MmsProvider.java, there is a possible way to arbitrarily delete files which affect telephony, SMS, and MMS functionalities due to a path traversal error. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	9.1

The following CVEs have medium severity score: CVE-2025-48587, CVE-2025-48585, CVE-2026-0024, CVE-2026-0005, CVE-2025-48642, CVE-2024-43766, CVE-2025-48631,

Google Play system updates
The following issues are included in Project Mainline components:

Subcomponent	CVE
Documents UI	CVE-2026-0013
MediaProvider	CVE-2025-48544, CVE-2025-48567, CVE-2025-48578, CVE-2025-48579, CVE-2025-48582
Media Codecs	CVE-2026-0006
MediaProvider	CVE-2026-0024, CVE-2026-0035
Permission Controller	CVE-2025-48653
Profiling	CVE-2025-48585, CVE-2025-48587

2026-03-05 security patch level vulnerability details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2026-03-05 patch level. Vulnerabilities are grouped under the component they affect. Issues are described in the tables below and include CVE ID, associated references, type of vulnerability, severity, and updated AOSP versions (where applicable). When available, we link the public change that addressed the issue to the bug ID, like the AOSP change list. When multiple changes relate to a single bug, additional references are linked to numbers following the bug ID.

Kernel

The most severe vulnerability in this section could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.

CVE ID	Description	CVSS Score
CVE-2026-0031	In multiple functions of mem_protect.c, 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.	8.4
CVE-2026-0030	In __host_check_page_state_range of mem_protect.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4
CVE-2026-0028	In __pkvm_host_share_guest of mem_protect.c, 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.	8.4
CVE-2026-0038	In multiple functions of mem_protect.c, there is a possible way to execute arbitrary code due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitati	8.4
CVE-2026-0037	In multiple functions of ffa.c, there is a possible memory corruption due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4
CVE-2025-38616	In the Linux kernel, the following vulnerability has been resolved: tls: handle data disappearing from under the TLS ULP TLS expects that it owns the receive queue of the TCP socket. This cannot be guaranteed in case the reader of the TCP socket entered before the TLS ULP was installed, or uses some non-standard read API (eg. zerocopy ones). Replace the WARN_ON() and a buggy early exit (which leaves anchor pointing to a freed skb) with real error handling. Wipe the parsing state and tell the reader to retry. We already reload the anchor every time we (re)acquire the socket lock, so the only condition we need to avoid is an out of bounds read (not having enough bytes in the socket for previously parsed record len). If some data was read from under TLS but there's enough in the queue we'll reload and decrypt what is most likely not a valid TLS record. Leading to some undefined behavior from TLS perspective (corrupting a stream? missing an alert? missing an attack?) but no kernel crash should take place.	7.1
CVE-2025-38618	In the Linux kernel, the following vulnerability has been resolved: vsock: Do not allow binding to VMADDR_PORT_ANY It is possible for a vsock to autobind to VMADDR_PORT_ANY. This can cause a use-after-free when a connection is made to the bound socket. The socket returned by accept() also has port VMADDR_PORT_ANY but is not on the list of unbound sockets. Binding it will result in an extra refcount decrement similar to the one fixed in fcdd2242c023 (vsock: Keep the binding until socket destruction). Modify the check in __vsock_bind_connectible() to also prevent binding to VMADDR_PORT_ANY.	7.8
CVE-2025-39682	In the Linux kernel, the following vulnerability has been resolved: tls: fix handling of zero-length records on the rx_list Each recvmsg() call must process either - only contiguous DATA records (any number of them) - one non-DATA record If the next record has different type than what has already been processed we break out of the main processing loop. If the record has already been decrypted (which may be the case for TLS 1.3 where we don't know type until decryption) we queue the pending record to the rx_list. Next recvmsg() will pick it up from	7.1

	there. Queuing the skb to rx_list after zero-copy decrypt is not possible, since in that case we decrypted directly to the user space buffer, and we don't have an skb to queue (darg.skb points to the ciphertext skb for access to metadata like length). Only data records are allowed zero-copy, and we break the processing loop after each non-data record. So we should never zero-copy and then find out that the record type has changed. The corner case we missed is when the initial record comes from rx_list, and it's zero length.	
CVE-2026-0029	In __pkvm_init_vm of pkvm.c, there is a possible memory corruption due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4
CVE-2026-0032	In multiple functions of mem_protect.c, there is a possible out-of-bounds write due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8

The following CVEs have medium severity score: CVE-2026-0027, CVE-2024-43859, CVE-2025-39946, CVE-2025-40266

Arm components

This vulnerability affects Arm components and further details are available directly from Arm. The severity assessment of this issue is provided directly by Arm.

CVE ID	Description	CVSS Score
CVE-2025-2879	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform improper GPU processing operations to expose sensitive data.This issue affects Valhall GPU Kernel Driver: from r29p0 through r49p4, from r50p0 through r54p0; Arm 5th Gen GPU Architecture Kernel Driver: from r41p0 through r49p4, from r50p0 through r54p0.	5.1

Imagination Technologies

These vulnerabilities affect Imagination Technologies components and further details are available directly from Imagination Technologies. The severity assessment of these issues is provided directly by Imagination Technologies.

CVE ID	Description	CVSS Score
CVE-2025-10865	Software installed and run as a non-privileged user may conduct improper GPU system calls to cause mismanagement of reference counting to cause a potential use after free. Improper reference counting on an internal resource caused scenario where potential for use after free was present.	7.8
CVE-2025-13952	A web page that contains unusual GPU shader code is loaded from the Internet into the GPU compiler process triggers a write use-after-free crash in the GPU shader compiler library. On certain platforms, when the compiler process has system privileges this could enable further exploits on the device. The shader code contained in the web page executes a path in the compiler that held onto an out of date pointer, pointing to a freed memory object.	9.8
CVE-2025-58407	Kernel or driver software installed on a Guest VM may post improper commands to the GPU Firmware to exploit a TOCTOU	7.4

	race condition and trigger a read and/or write of data outside the allotted memory escaping the virtual machine.	
CVE-2025-58408	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger reads of stale data that can lead to kernel exceptions and write use-after-free. The Use After Free common weakness enumeration was chosen as the stale data can include handles to resources in which the reference counts can become unbalanced. This can lead to the premature destruction of a resource while in use.	5.9
CVE-2025-58409	Software installed and run as a non-privileged user may conduct improper GPU system calls to subvert GPU HW to write to arbitrary physical memory pages. Under certain circumstances this exploit could be used to corrupt data pages not allocated by the GPU driver but memory pages in use by the kernel and drivers running on the platform altering their behaviour. This attack can lead the GPU to perform write operations on restricted internal GPU buffers that can lead to a second order affect of corrupted arbitrary physical memory.	3.5
CVE-2025-58411	Software installed and run as a non-privileged user may conduct improper GPU system calls to cause mismanagement of resources reference counting creating a potential use after free scenario. Improper resource management and reference counting on an internal resource caused scenario where potential write use after free was present.	8.8

The following CVE have high severity and have not yet been documented or assigned a score: CVE-2026-21735

MediaTek components

These vulnerabilities affect MediaTek components and further details are available directly from MediaTek. The severity assessment of these issues is provided directly by MediaTek.

CVE ID	Description	CVSS Score
CVE-2025-20795	In KeyInstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10276761; Issue ID: MSV-5141.	7.8
CVE-2026-20425	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10320471; Issue ID: MSV-5539.	6.7
CVE-2026-20426	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10320471; Issue ID: MSV-5538.	6.7
CVE-2026-20427	In display, there is a possible escalation of privilege due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10320471; Issue ID: MSV-5537.	6.7
CVE-2026-20428	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10320471; Issue ID: MSV-5536.	6.7

CVE-2026-20434	In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: MOLY00782946; Issue ID: MSV-4135.	7.5
CVE-2025-20760	In Modem, there is a possible read of uninitialized heap data due to an uncaught exception. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01676750; Issue ID: MSV-4653.	6.5
CVE-2025-20761	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01311265; Issue ID: MSV-4655.	6.5
CVE-2025-20762	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01685181; Issue ID: MSV-4760.	6.5
CVE-2025-20793	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01430930; Issue ID: MSV-4836.	6.5
CVE-2025-20794	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01689259 / MOLY01586470; Issue ID: MSV-4847.	6.5
CVE-2026-20401	In Modem, there is a possible system crash due to an uncaught exception. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01738310; Issue ID: MSV-5933.	7.5
CVE-2026-20401	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00693083; Issue ID: MSV-5928.	6.5
CVE-2026-20402	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00693083; Issue ID: MSV-5928.	6.5
CVE-2026-20403	In Modem, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01689254 (Note: For N15 and NR16) / MOLY01689259 (Note: For NR17 and NR17R); Issue ID: MSV-4843.	6.5

CVE-2026-20404	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01689248; Issue ID: MSV-4837.	6.5
CVE-2026-20405	In Modem, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01688495; Issue ID: MSV-4818.	6.5
CVE-2026-20406	In Modem, there is a possible system crash due to an uncaught exception. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01726634; Issue ID: MSV-5728.	6.5
CVE-2026-20420	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01738313; Issue ID: MSV-5935.	6.5
CVE-2026-20421	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01738293; Issue ID: MSV-5922.	6.5
CVE-2026-20422	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00827332; Issue ID: MSV-5919.	6.5

Misc OEM

This vulnerability affects Misc OEM components and further details are available directly from Misc OEM. The severity assessment of this issue is provided directly by Misc OEM.

CVE ID	Description	CVSS Score
CVE-2025-48613	In VBMeta, there is a possible way to modify and resign VBMeta using a test key, assuming the original image was previously signed with the same key. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8

Unisoc components

These vulnerabilities affect Unisoc components and further details are available directly from Unisoc. The severity assessment of these issues is provided directly by Unisoc.

The following CVE have high severity and have not yet been documented or assigned a score: CVE-2025-61612, CVE-2025-61613, CVE-2025-61614, CVE-2025-61615, CVE-2025-61616, CVE-2025-69278, CVE-2025-69279

Qualcomm components

These vulnerabilities affect Qualcomm components and are described in further detail in

the appropriate Qualcomm security bulletin or security alert. The severity assessment of these issues is provided directly by Qualcomm.

CVE ID	Description	CVSS Score
CVE-2025-47388	Memory corruption while passing pages to DSP with an unaligned starting address.	7.8
CVE-2025-47394	Memory corruption when copying overlapping buffers during memory operations due to incorrect offset calculations.	7.8
CVE-2025-47396	Memory corruption occurs when a secure application is launched on a device with insufficient memory.	7.8
CVE-2025-47397	Memory Corruption when initiating GPU memory mapping using scatter-gather lists due to unchecked IOMMU mapping errors.	7.8
CVE-2025-47398	Memory Corruption while deallocating graphics processing unit memory buffers due to improper handling of memory pointers.	7.8
CVE-2025-59600	Memory Corruption when adding user-supplied data without checking available buffer space.	7.8
CVE-2026-21385	Memory corruption while using alignments for memory allocation.	7.8

Qualcomm closed-source components

These vulnerabilities affect Qualcomm closed-source components and are described in further detail in the appropriate Qualcomm security bulletin or security alert. The severity assessment of these issues is provided directly by Qualcomm.

CVE ID	Description	CVSS Score
CVE-2025-47339	Memory corruption while deinitializing a HDCP session.	7.8
CVE-2025-47346	Memory corruption while processing a secure logging command in the trusted application.	7.8
CVE-2025-47348	Memory corruption while processing identity credential operations in the trusted application.	7.8
CVE-2025-47366	Cryptographic issue when a Trusted Zone with outdated code is triggered by a HLOS providing incorrect input.	7.8
CVE-2025-47378	Cryptographic Issue when a shared VM reference allows HLOS to boot loader and access cert chain.	7.1
CVE-2025-47385	Memory Corruption when accessing trusted execution environment without proper privilege check.	7.8
CVE-2025-47395	Transient DOS while parsing a WLAN management frame with a Vendor Specific Information Element.	6.5
CVE-2025-47402	Transient DOS when processing a received frame with an excessively large authentication information element.	6.5

Affected Products

- Android OS devices with security patch levels prior to 2026-03-05
- Patch level 2026-03-01 addresses the issues listed under the 2026-03-01 section.
- Patch level 2026-03-05 addresses all issues in both 2026-03-01 and 2026-03-05 sections and all previous patch levels.

Recommendations

Smarttech247 team recommends the following actions to be taken:

- Apply the appropriate patches or appropriate mitigations immediately after appropriate testing.

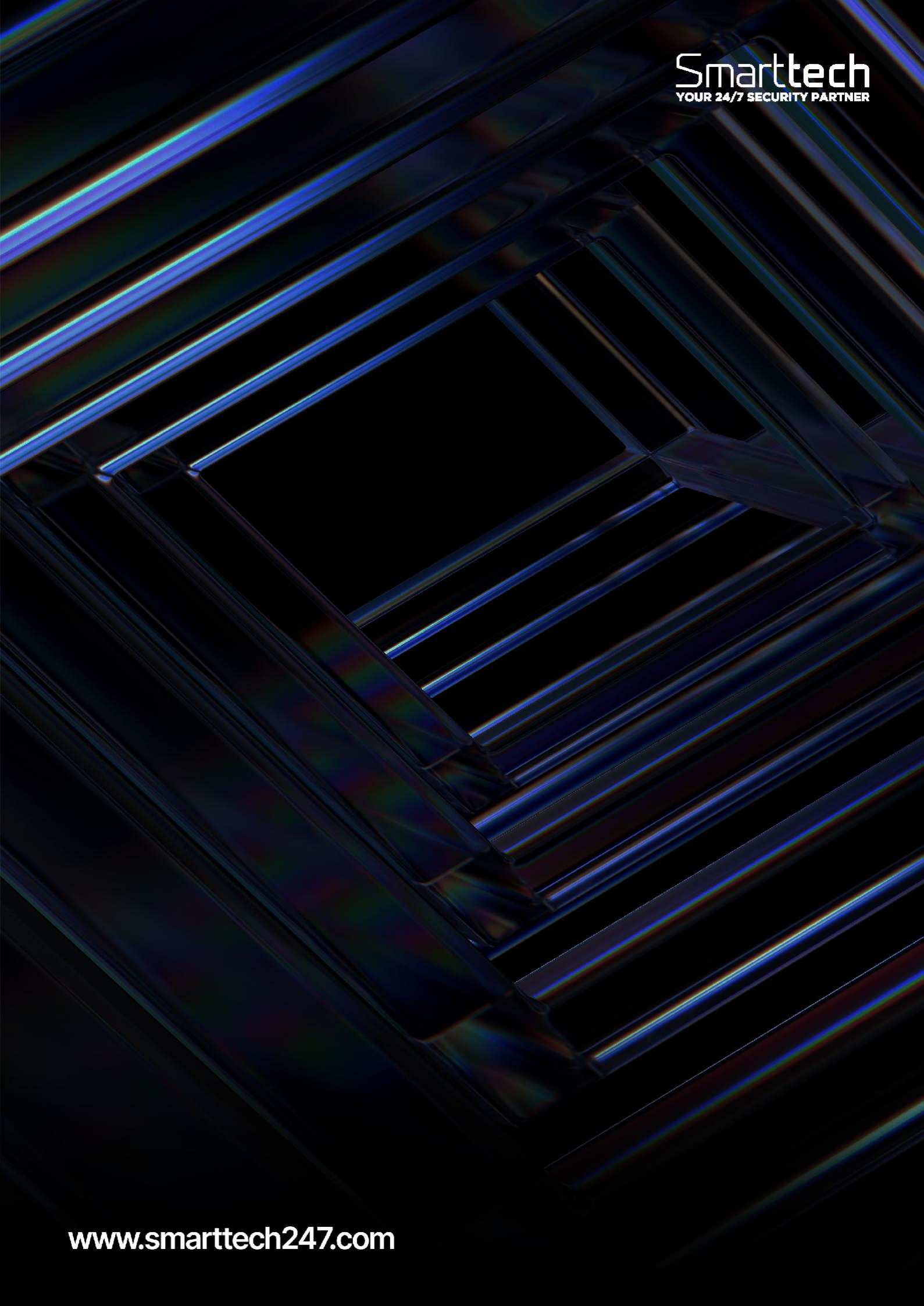
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Use the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.
- Apply the Principle of Least Privilege to all systems and services.
- Apply advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.
- Kindly ensure that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.

References

https://source.android.com/docs/security/bulletin/2026/2026-03-01#framework

CVE

CVE-2025-32313, CVE-2025-48544, CVE-2025-48567, CVE-2025-48568, CVE-2025-48574, CVE-2025-48577, CVE-2025-48578, CVE-2025-48579, CVE-2025-48582, CVE-2025-48605, CVE-2025-48619, CVE-2025-48630, CVE-2025-48634, CVE-2025-48635, CVE-2025-48644, CVE-2025-48645, CVE-2025-48646, CVE-2025-48654, CVE-2026-0007, CVE-2026-0008, CVE-2026-0010, CVE-2026-0011, CVE-2026-0012, CVE-2026-0013, CVE-2026-0014, CVE-2026-0015, CVE-2026-0020, CVE-2026-0023, CVE-2026-0025, CVE-2026-0026, CVE-2026-0034, CVE-2026-0047, CVE-2024-43766, CVE-2025-48585, CVE-2025-48587, CVE-2025-48602, CVE-2025-48609, CVE-2025-48631, CVE-2025-48641, CVE-2025-48642, CVE-2025-48650, CVE-2025-48653, CVE-2025-64783, CVE-2025-64784, CVE-2025-64893, CVE-2026-0005, CVE-2026-0006, CVE-2026-0017, CVE-2026-0021, CVE-2026-0024, CVE-2026-0035, CVE-2024-43859, CVE-2025-38616, CVE-2025-38618, CVE-2025-39682, CVE-2025-39946, CVE-2025-40266, CVE-2026-0027, CVE-2026-0028, CVE-2026-0029, CVE-2026-0030, CVE-2026-0031, CVE-2026-0032, CVE-2026-0037, CVE-2026-0038, CVE-2025-2879, CVE-2025-10865, CVE-2025-13952, CVE-2025-58407, CVE-2025-58408, CVE-2025-58409, CVE-2025-58411, CVE-2026-21735, CVE-2025-20760, CVE-2025-20761, CVE-2025-20762, CVE-2025-20793, CVE-2025-20794, CVE-2025-20795, CVE-2026-20401, CVE-2026-20402, CVE-2026-20403, CVE-2026-20404, CVE-2026-20405, CVE-2026-20406, CVE-2026-20420, CVE-2026-20421, CVE-2026-20422, CVE-2026-20425, CVE-2026-20426, CVE-2026-20427, CVE-2026-20428, CVE-2026-20434, CVE-2025-61612, CVE-2025-61613, CVE-2025-61614, CVE-2025-61615, CVE-2025-61616, CVE-2025-69278, CVE-2025-69279, CVE-2025-47388, CVE-2025-47394, CVE-2025-47396, CVE-2025-47397, CVE-2025-47398, CVE-2025-59600, CVE-2026-21385, CVE-2025-47339, CVE-2025-47346, CVE-2025-47348, CVE-2025-47366, CVE-2025-47378, CVE-2025-47385, CVE-2025-47395, CVE-2025-47402


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com