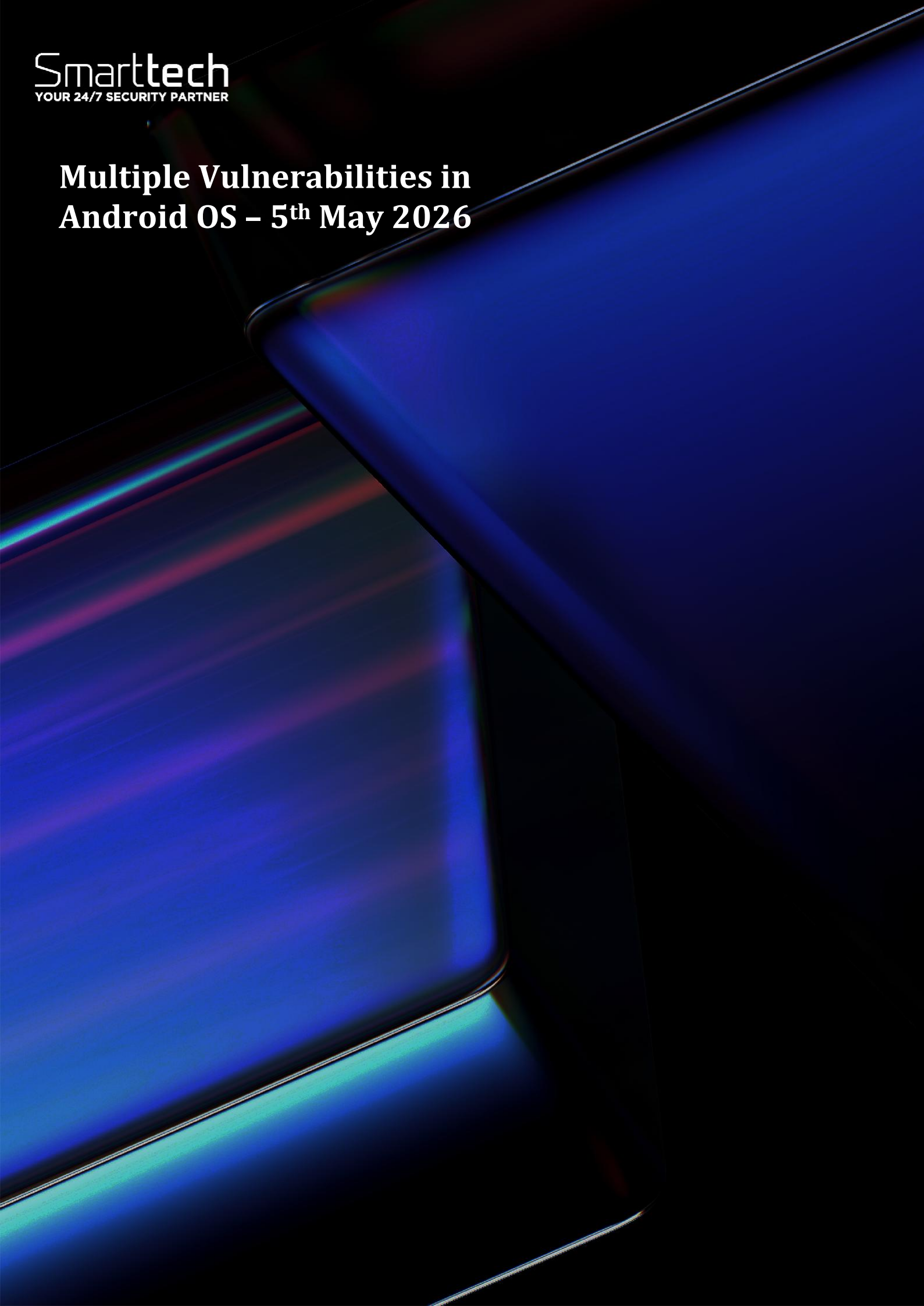
Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Android OS – 5th May 2026



Document ID	SMA-Informative Cyber Alert
Document status	ISSUED
Authors	Alex Ciuta <alexandru.ciuta@smarttech247.com>
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	5th May 2026
Issue Date	5th May 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

A new vulnerability has been identified in the Google Android operating system, including an issue in the wireless ADB authentication mechanism. Android is a mobile operating system developed by Google and used across smartphones, tablets, wearables, and other devices. Successful exploitation of this vulnerability may allow an attacker on a proximal or adjacent network to bypass mutual authentication and execute code remotely as the shell user. Because the attack requires no user interaction and grants command execution under the shell account, an attacker could perform actions permitted to that user, such as accessing limited system information or interacting with debugging interfaces.

Technical Summary

2026-05-01 security patch level vulnerability details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2026-05-01 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.

System

User interaction is not needed for exploitation.

CVE ID	Description	CVSS Score
CVE-2026-0073	In adbd_tls_verify_cert of auth.cpp, there is a possible bypass of wireless ADB mutual authentication due to a logic error in the code. This could lead to remote (proximal/adjacent) code execution as the shell user with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8

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

Subcomponent	CVE
adbd	CVE-2026-0073

Affected Products

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

Recommendations

Smarttech247 team recommends the following actions to be taken:

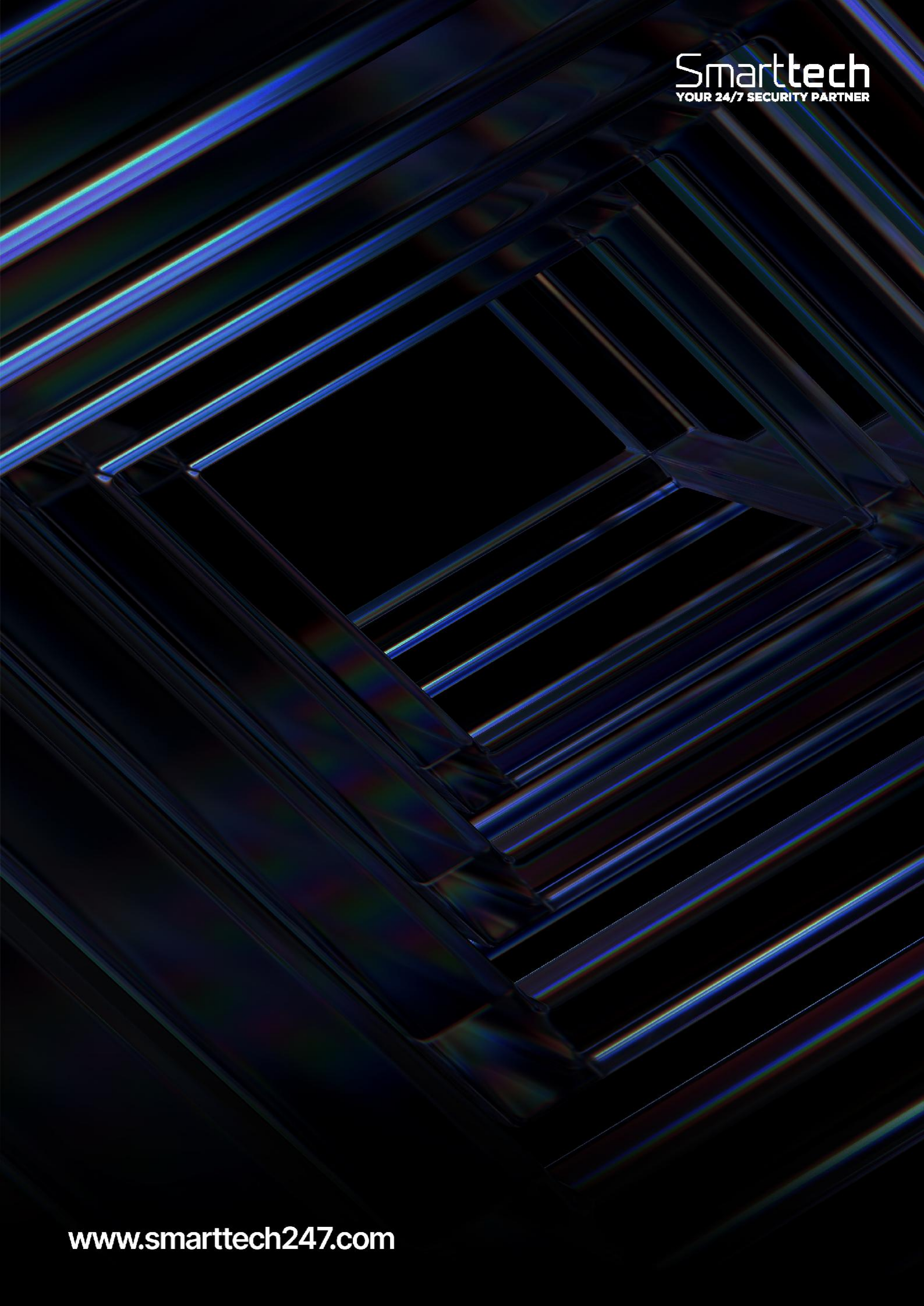
- Apply the appropriate patches or appropriate mitigations immediately after appropriate testing.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Use the right Vulnerability Management Tools to assess endpoint, networks or applications 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/2026/2026-05-01

CVE

CVE-2026-0073


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