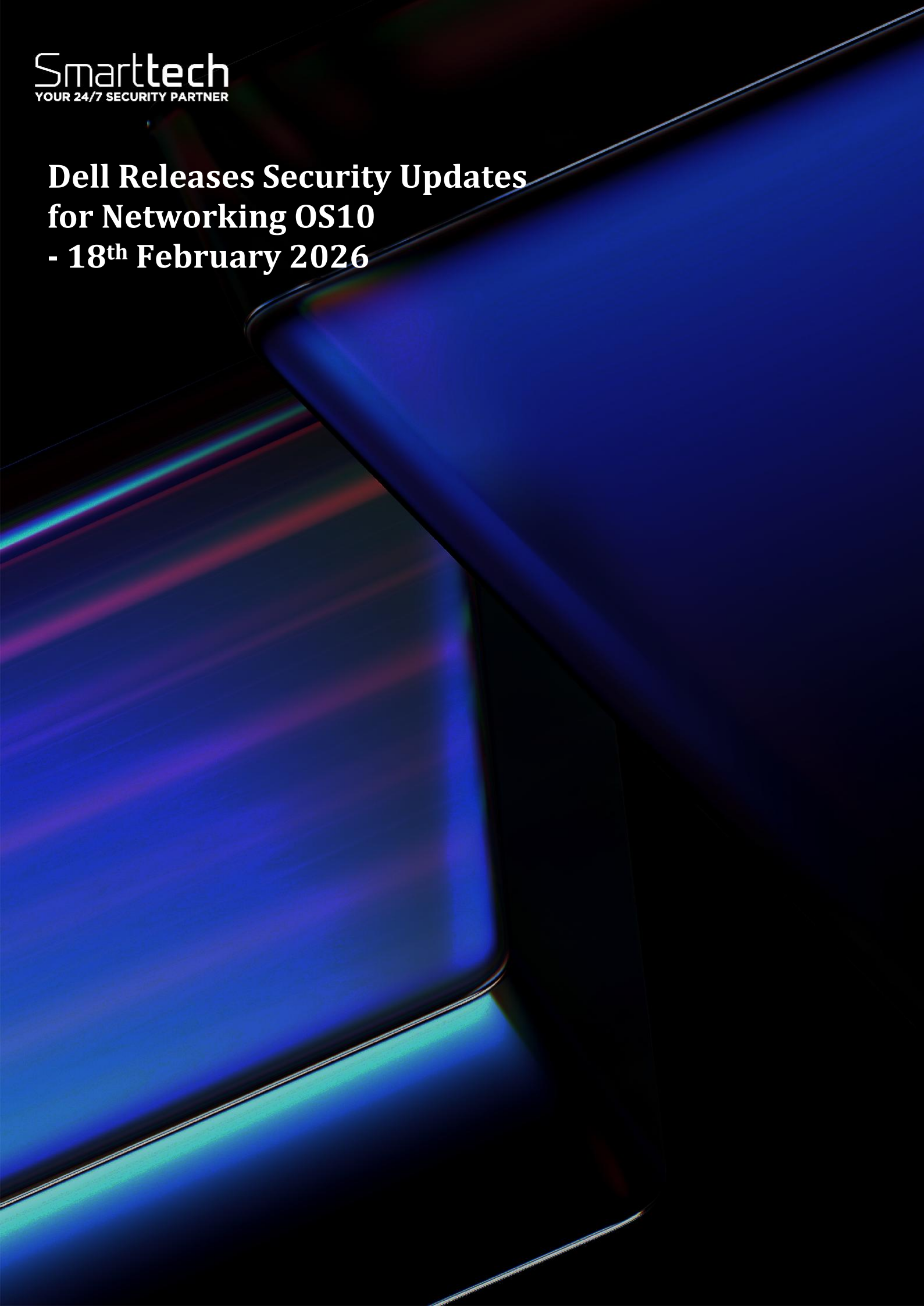
Smarttech
YOUR 24/7 SECURITY PARTNER

Dell Releases Security Updates for Networking OS10 - 18th February 2026



Document ID	SMA-Informative Cyber Alert
Document status	ISSUED
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	18th February 2026
Issue Date	18th February 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 security vulnerabilities have been identified in Dell Networking OS10. Successful exploitation of these vulnerabilities by malicious users could allow compromise of affected systems, potentially leading to remote code execution, command execution, memory corruption or denial of service (DoS). Remediation is available through updated OS10 software releases to address these issues.

Technical Summary

Proprietary Code CVEs	Description	CVSS Base Score
CVE-2026-22284	Dell SmartFabric OS10 Software, versions prior to 10.5.5.17 and 10.5.6.12, contains an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	6.6

Third-party Component	CVEs
redis	CVE-2025-46817, CVE-2025-46819, CVE-2025-49844
libfcgi	CVE-2025-23016
openssh (pkix-ssh)	CVE-2025-61984
libxml2	CVE-2025-9714, CVE-2025-7425
nginx	CVE-2024-7347, CVE-2024-33452, CVE-2025-23419
libssh	CVE-2020-16135, CVE-2023-6004, CVE-2023-6918
libpng1.6	CVE-2025-64505, CVE-2025-64506, CVE-2025-64720, CVE-2025-65018, CVE-2025-66293
glib2.0	CVE-2025-4373, CVE-2025-7039, CVE-2025-13601, CVE-2025-14087, CVE-2025-14512

Affected Products & Remediation

Product	Affected Versions	Remediated Versions
Dell Networking OS10	Versions prior to 10.5.5.17	Version 10.5.5.17
	Versions prior to 10.5.6.12	Version 10.5.6.12

Recommendations

Smarttech247 team recommends the following actions to be taken:

- Upgrade to the latest versions in order to obtain a fix for these vulnerabilities.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Apply the Principle of Least Privilege to all systems and services.

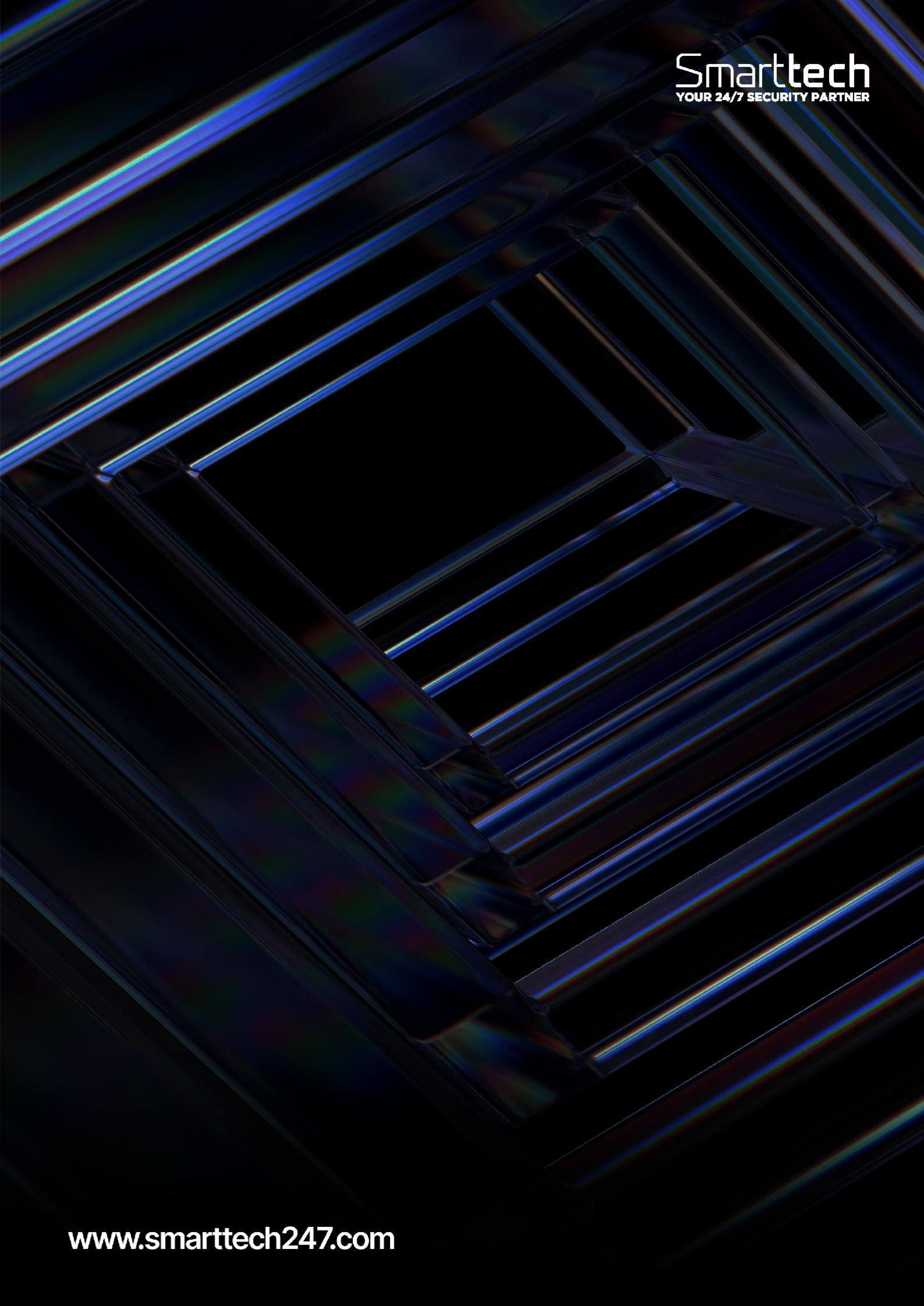
References

1. https://www.dell.com/support/kbdoc/en-us/000429176/dsa-2026-032-security-update-for-dell-networking-os10-vulnerabilities
2. https://www.dell.com/support/kbdoc/en-us/000429181/dsa-2026-033-security-update-for-dell-networking-os10-vulnerabilities
3. https://www.benasin.space/2025/03/18/OpenResty-lua-nginx-module-v0-10-26-HTTP-Request-Smuggling-in-HEAD-requests/
4. https://www.wiz.io/blog/wiz-research-redis-rce-cve-2025-49844
5. https://redrays.io/blog/poc-for-cve-2025-49844-cve-2025-46817-and-cve-2025-46818-critical-lua-engine-vulnerabilities/
6. https://github.com/dantsco/CVE-2025-64720-PoC
7. https://github.com/pnggroup/libpng/security/advisories/GHSA-7wv6-48j4-hj3g
8. https://nvd.nist.gov/
9. https://www.cisa.gov/

CVEs:

CVE-2025-46817
CVE-2025-46819
CVE-2025-49844
CVE-2025-23016
CVE-2025-61984
CVE-2025-9714
CVE-2025-7425
CVE-2024-7347
CVE-2024-33452
CVE-2025-23419
CVE-2020-16135
CVE-2023-6004
CVE-2023-6918
CVE-2025-64505
CVE-2025-64506
CVE-2025-64720
CVE-2025-65018
CVE-2025-66293
CVE-2025-4373
CVE-2025-7039
CVE-2025-13601

CVE-2025-14087
CVE-2025-14512
CVE-2026-22284


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