

Daily insight report

Last updated: 2026-10-13

Date	2026-10-13
Key items	6 key items (5 auto-verified, 1 listed), 0 high-risk, 3 medium-high, 0 jurisdictions

Key items today

1

⚠ Medium-high

✓ Passed 3-level verification (automated)

✓ High

CVE-2026-108804 (<https://nvd.nist.gov/vuln/detail/CVE-2026-108804>)
CVSS 10.0 (NVD record)

The web management backend of TRENDnet TEW-751DR, TEW-752DRU, and TEW733GR has an operating system command injection vulnerability. It is recommended to check for affected devices promptly and take mitigation measures.

Why it matters:

The vulnerability is located in the web management backend, and manipulating a parameter can lead to command injection, which may allow the device to be taken over. The affected models and firmware versions are 1.03B01/1.03B03. The source does not state whether a patch is available or whether the vulnerability has been exploited in practice. *Unconfirmed*

Recommended actions:

Check whether TEW-751DR, TEW-752DRU, or TEW733GR devices are deployed in the network, and confirm whether the firmware version is 1.03B01 or 1.03B03.

Provenance

2

 **Medium-high** **Passed 3-level verification (automated)** **High****CVE-2026-108894** (<https://nvd.nist.gov/vuln/detail/CVE-2026-108894>)

CVSS 9.9 (NVD record)

A security flaw has been found in the static route handling component of Linksys E1700 1.0.0.4.003, involving the addStaticRoute function. Impact and exploitation details. *Unconfirmed*

Why it matters:

The affected part is the web management interface parameter handling in the router firmware. Vendors and operators should promptly verify device models and versions. Severity, exploitability, and patch status are not stated in the source. *Unconfirmed*

Recommended actions:

Check whether the network contains devices running Linksys E1700 1.0.0.4.003 firmware

Provenance

3

 **Medium-high** **Passed 3-level verification (automated)** **High****CVE-2026-108929** (<https://nvd.nist.gov/vuln/detail/CVE-2026-108929>)

CVSS 9.9 (NVD record)

A parameter injection vulnerability exists in the DDNS component of Netcore NR268 1.7.121109 and can be exploited remotely. Immediate review and mitigation of exposure are recommended.

Why it matters:

The vulnerability resides in the router's DDNS configuration interface, and attacks can be launched remotely, potentially affecting devices deployed by carriers and enterprises. The source currently does not state patch status, exploitation status, or scope of impact, so these must be assessed independently. *Unconfirmed*

Recommended actions:

Inventory devices in the network running Netcore NR268 1.7.121109

Provenance

4

 Medium Passed 3-level verification (automated) High**CVE-2026-103903** (<https://nvd.nist.gov/vuln/detail/CVE-2026-103903>)

CVSS 8.8 (NVD record)

The WinBox authentication process in RouterOS has an improper authorization issue that allows a low-privileged authenticated attacker to obtain the authorization policies of other accounts.

Why it matters:

If carriers and equipment vendors expose WinBox in their networks, an attacker holding low-privileged credentials could use this issue to learn the permission policies of other accounts, which may provide information for subsequent privilege escalation or lateral movement. The affected versions and fixed versions are not stated in the source. *Unconfirmed*

Recommended actions:

Review all RouterOS devices in the network that have WinBox enabled, and identify which low-privileged accounts are allowed to use WinBox

Provenance

5

 Medium High**CVE-2026-108906** (<https://nvd.nist.gov/vuln/detail/CVE-2026-108906>)

CVSS 7.2 (NVD record)

Provenance

6

 Medium Passed 3-level verification (automated) High**CVE-2026-108980** (<https://nvd.nist.gov/vuln/detail/CVE-2026-108980>)

CVSS 8.8 (NVD record)

The plugin installation feature in Blinko 1.8.8 and earlier versions has a directory traversal vulnerability that allows any authenticated user to overwrite startup files as root.

Why it matters:

The plugin name is used to construct the installation path without sanitization, and the related endpoint is open to any authenticated user, which may allow startup files to be overwritten with root privileges. Operators should investigate promptly and restrict access. The fixed version and actual exploitation are not stated in the source. *Unconfirmed*

Recommended actions:

Immediately review all Blinko deployments and confirm whether the version is 1.8.8 or earlier.

Provenance

Scores and risk labels are our own assessment, based on public sources as of the date shown. They are opinions, not findings or statements of fact about any government, organisation or group.

Deep focus

☐ No deep-focus item today.

Watch tomorrow

☐ Nothing to watch tomorrow yet.

For information only; this is not legal advice.

Auto-generated and automatically verified; not reviewed by human analysts or external experts

CyberInsight Asia · contact@cyberinsight.info

CyberInsight Asia · <https://www.cyberinsight.info>