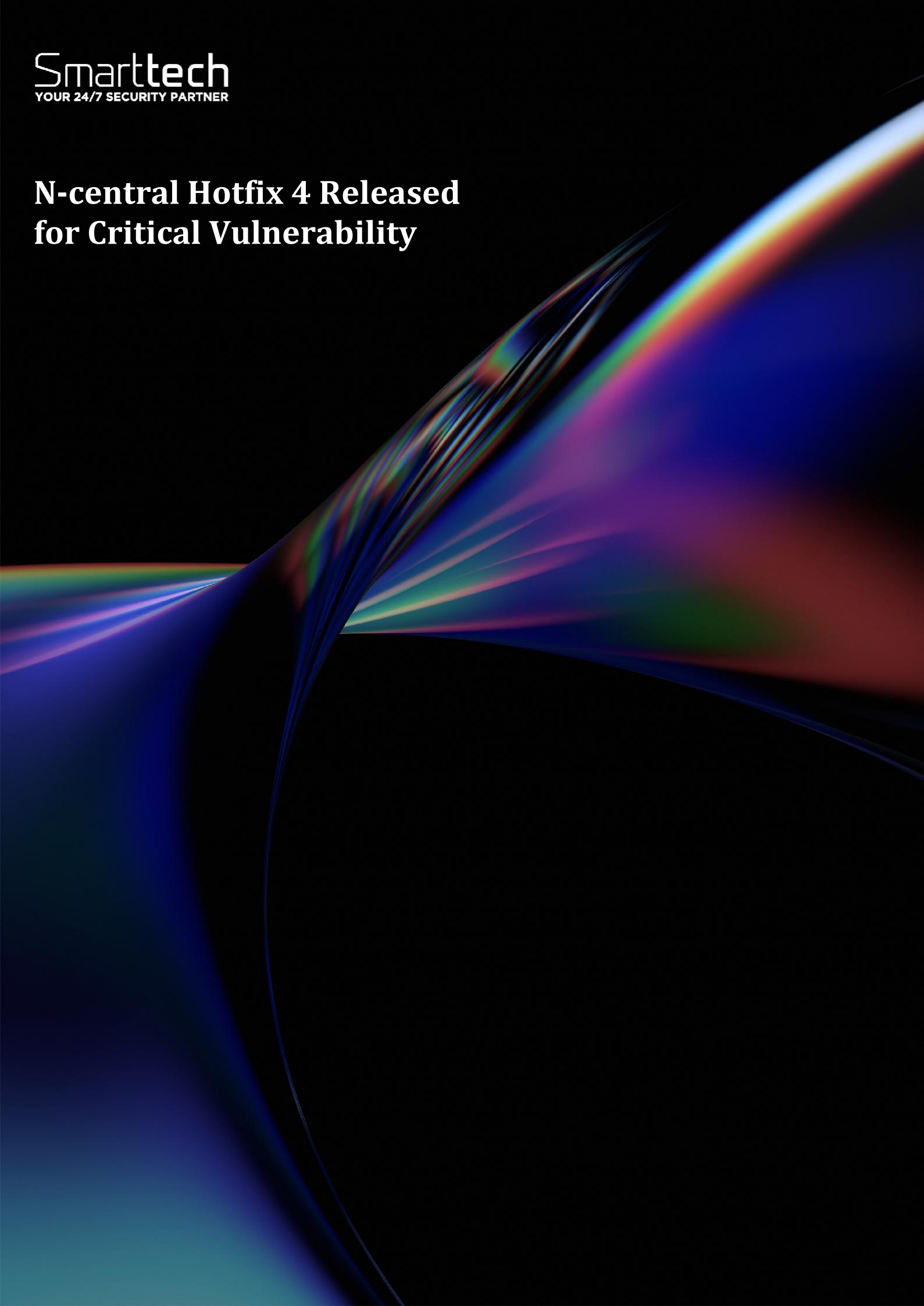
Smarttech
YOUR 24/7 SECURITY PARTNER

N-central Hotfix 4 Released for Critical Vulnerability



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	152
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-08
Issue Date	2026-09-06

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

N-able has released a fourth hotfix for N-central, addressing CVE-2026-86218, a critical vulnerability that could allow unauthenticated remote code execution on on-premises N-central servers. The security update is intended for on-premises deployments, while N-central hosted instances (NCOD) have already been patched by N-able.

Risk:

Government:

- Large and medium government entities: Critical
- Small government entities: Critical

Businesses:

- Large and medium business entities: Critical
- Small business entities: Critical

Technical summary:

CVE	*Description*
CVE-2026-86218 **CVSS Score: 10**	N-central is vulnerable to a pre-authenticated remote code execution.

Affected Products:

Product	*Version*
N-Central	Prior to 2026.3.1.14

Recommendations

We recommend the following actions be taken:

- Apply N-central 2026.3 Hotfix 4 (build 2026.3.1.14) immediately to protect affected on-premises environments.
- 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.
- Ensure that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.

References

https://status.n-able.com/2026/09/06/n-central-2026-3-hotfix-4-cve-2026-86218/

CVEs

CVE-2026-86218

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com