Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0478

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in N-able N-central

Publicatiedatum: 11-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

N-able heeft meerdere kwetsbaarheden verholpen in N-able N-central. Deze kwetsbaarheden treffen versies ouder dan 2026.4.1.26.

Duiding

Er meerdere kwetsbaarheden met betrekking tot XML External Entity (XXE), waardoor de verwerking van XML-data mogelijk op ongewenste wijze kan worden beïnvloed. Daarnaast zijn er kwetsbaarheden in de vorm van OGNL Injection en Stored Cross-Site Scripting (XSS), waarbij kwaadaardige code kan worden geïnjecteerd en uitgevoerd binnen de webinterface, waaronder in de context van een administrator.

Verder zijn er meerdere kwetsbaarheden die lokale privilege-escalatie mogelijk maken, waaronder via een onjuist beveiligde syslog-ng-configuratie en onveilige Inter-Process Communication (IPC)-kanalen. Ook is er sprake van een Server-Side Request Forgery (SSRF)-kwetsbaarheid via de validatie van schema-informatie bij het importeren van services. Ten slotte is een kwetsbaarheid vastgesteld in de verwerking van bestandspaden bij het uploaden naar de file repository, waarbij path traversal kan leiden tot Remote Code Execution (RCE).

Oplossingen

N-able heeft N-central 2026.4 HF2 (build 2026.4.1.26) uitgebracht, waarin de betreffende kwetsbaarheden zijn verholpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://status.n-able.com/2026/11/10/n-central-2026-4-hf2-release-notes/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-125883	9.3 CRITICAL
CVE-2026-125878	8.7 HIGH
CVE-2026-125879	8.6 HIGH
CVE-2026-125880	8.3 HIGH
CVE-2026-125881	9.3 CRITICAL
CVE-2026-125882	8.6 HIGH
CVE-2026-91000	8.4 HIGH

CWE's

CWE	Beschrijving
CWE-23	Relative Path Traversal
CWE-79	Improper Neutralization of Input During Web Page Generation
CWE-266	Incorrect Privilege Assignment
CWE-306	Missing Authentication for Critical Functionality
CWE-611	Improper Restriction of XML External Entity Reference
CWE-644	Improper Neutralization of HTTP Headers for Scripting Syntax
CWE-918	Server-Side Request Forgery

Getroffen producten

N-able
N-central

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:
NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.