



NCSC-2026-0342

Kwetsbaarheid verholpen in N-central van N-able

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 07-09-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het 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 delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

N-able heeft een kwetsbaarheid verholpen in N-central versies eerder dan 2026.3.1.14.

Duiding

De kwetsbaarheid betreft een pre-authenticatie remote code execution flaw. Een aanvaller kan hierdoor op afstand willekeurige code uitvoeren op het getroffen systeem zonder enige vorm van authenticatie. Alle installaties die draaien op de kwetsbare versies van N-central zijn getroffen. Klanten met een on-premises N-central-omgeving wordt geadviseerd zo snel mogelijk te upgraden naar N-central 2026.3 HF4. Voor gebruikers van een gehoste N-central-instantie (NCOD) zijn de patches al toegepast. Er is op dit moment geen actie vereist.

N-able meldt dat pogingen tot exploitatie zijn waargenomen, volg het advies van N-able op om onderzoek te doen naar IoC's.

Oplossingen

N-able heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://documentation.n-able.com/N-central/Release_Notes/GA/Content/N-central_2026.3_HF4_Release_Notes.htm
- <https://me.n-able.com/s/security-advisory/aArVy0000002Ld3KAE/cve202686218-preauthentication-remote-code-execution>
- <https://www.n-able.com/blog/n-central-security-hotfix-september-5-2026>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-86218	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-96	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')

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.