Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0275

Kwetsbaarheden verholpen in N-able N-central

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 07-08-2026
Revisie: 1.0.1

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

Update Revisie 1

N-able heeft een additionele Hotfix (2026.3.1.10) gedeeld voor CVE-2026-18577.

Feiten

N-able heeft kwetsbaarheden verholpen in N-able N-central tot en met versie 2026.3.1.

Duiding

De kwetsbaarheden betreffen bypass van authenticatie in N-able N-central. In versies tot en met 2026.1 kan een aanvaller de authenticatiecontroles omzeilen door een alternatieve route binnen de applicatie te benutten.

In versies tot en met 2026.3.1 is een onvolledige patch voor de kwetsbaarheid met kenmerk CVE-2026-18556 geïntroduceerd die authenticatieomzeiling en overname van accounts mogelijk maakt. Dit issue heeft kenmerk CVE-2026-18577 toegewezen gekregen. Hierdoor kan een aanvaller ongeautoriseerd toegang krijgen tot gebruikersaccounts en het systeem controleren. Alle implementaties die de genoemde versies gebruiken, zijn kwetsbaar.

N-able meldt dat misbruik van de kwetsbaarheid is ontdekt en hierop gebruikers heeft geïnformeerd.

Oplossingen

N-able heeft Hotfix 2026.3.1.7 uitgebracht om de kwetsbaarheden te verhelpen en adviseert om de hotfix zo spoedig mogelijk in te zetten. Zie bijgevoegde referenties voor meer informatie.

Update:

N-able heeft aanvullend Hotfix 2026.3.1.10 uitgebracht die extra hardening bevat en adviseert deze zo snel mogelijk aanvullend aan de eerdere hotfix te installeren. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://documentation.n-able.com/N-central/Release_Notes/GA/Content/N-central_2026.3_HF1_Release_Notes.htm
- https://status.n-able.com/2026/08/06/n-central-2026-3-hotfix-2-additional-mitigation-for-cve-2026-18577/
- https://uptime.n-able.com/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-18577	8.2 HIGH
CVE-2026-18556	8.2 HIGH

CWE's

CWE	Beschrijving
CWE-287	Improper Authentication
CWE-288	Authentication Bypass Using an Alternate Path or Channel

Getroffen producten

N-able
N-central

Disclaimer