Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0399

Kwetsbaarheid verholpen in HPE OneView Software

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 24-12-2025
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

PoC vrijgegeven en verwerkt in een metasploit module.

Feiten

HPE heeft een kwetsbaarheid verholpen in de HPE OneView Software.

Duiding

De kwetsbaarheid bevindt zich in de manier waarop de OneView Software omgaat met externe verzoeken. Als HPE OneView Software via het internet toegankelijk is kunnen ongeauthenticeerde gebruikers op afstand code uitvoeren. Dit kan aanvallers in staat stellen controle te verkrijgen over de getroffen omgevingen.

Onderzoekers hebben Proof-of-Concept-code (PoC) gepubliceerd en verwerkt in een Metasploit-module. Het risico op scanverkeer en pogingen tot misbruik neemt hierdoor toe.

Oplossingen

Upgrade naar versie 11.0 of installeer een van de hotfixes die HPE heeft uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Het is wenselijk om dergelijke producten niet aan het internet bloot te stellen om aanvallen te voorkomen. Maak deze alleen toegankelijk vanaf vertrouwde systemen of maak gebruik van een VPN.

Referenties

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04985en_us&docLocale=en_US

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-37164	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-94	Improper Control of Generation of Code ('Code Injection')

Getroffen producten

HPE
HPE OneView

Disclaimer