



NCSC-2026-0339

Kwetsbaarheden verholpen in HPE Networking Fabric Composer

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 03-09-2026

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

HPE heeft meerdere kwetsbaarheden verholpen in HPE Networking Fabric Composer.

Duiding

De kwetsbaarheden in HPE Networking Fabric Composer betreffen onder andere authenticatiebypasses, privilege-escalaties, remote code execution, command injection, cross-site scripting (XSS), denial-of-service, arbitrary file write, path traversal, en onbevoegde toegang tot gevoelige informatie. Sommige kwetsbaarheden kunnen door ongeauthenticeerde aanvallers op afstand worden misbruikt, terwijl andere exploitatie vereisen door geauthenticeerde gebruikers met beperkte privileges. Exploitatie kan leiden tot het verkrijgen van administratieve toegang, het uitvoeren van willekeurige commando's met verhoogde privileges, het wijzigen van systeemconfiguraties, het uitlekken van gevoelige data, en het verstoren van de normale werking van het systeem. Diverse kwetsbaarheden zijn aanwezig in de API, het onderliggende besturingssysteem en de webgebaseerde managementinterface van het product. Sommige aanvallen vereisen dat de aanvaller zich op een aangrenzend netwerk bevindt of lokale toegang heeft. De kwetsbaarheden beïnvloeden de integriteit, vertrouwelijkheid en beschikbaarheid van het systeem en de netwerkfabric-omgeving die door HPE Networking Fabric Composer wordt beheerd.

Als de SSH beheerinterface publiekelijk via het internet bereikbaar is, kan CVE-2026-76658 door ongeautoriseerde aanvallers van buitenaf worden misbruikt voor volledige overname van het achterliggende datacenter-netwerk. Het is goed gebruik een dergelijk beheerinterface niet direct aan het internet te ontsluiten of af te schermen middels een VPN of whitelist.

Oplossingen

HPE heeft updates uitgebracht om de kwetsbaarheden in HPE Networking Fabric Composer te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05133en_us&docLocale=en_US

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-76657	10.0 CRITICAL
➤ CVE-2026-76658	10.0 CRITICAL

> CVE-2026-19766	9.6 CRITICAL
> CVE-2026-73700	9.0 CRITICAL
> CVE-2026-73701	9.0 CRITICAL
> CVE-2026-73702	8.8 HIGH
> CVE-2026-73703	8.8 HIGH
> CVE-2026-73704	8.8 HIGH
> CVE-2026-73705	8.8 HIGH
> CVE-2026-73706	8.6 HIGH
> CVE-2026-73707	8.5 HIGH
> CVE-2026-73708	8.3 HIGH
> CVE-2026-73709	8.3 HIGH
> CVE-2026-73710	8.2 HIGH
> CVE-2026-73711	8.1 HIGH
> CVE-2026-73713	7.8 HIGH
> CVE-2026-73714	7.6 HIGH
> CVE-2026-73716	7.5 HIGH
> CVE-2026-73717	7.5 HIGH
> CVE-2026-73718	7.4 HIGH
> CVE-2026-73719	7.2 HIGH
> CVE-2026-73720	7.2 HIGH
> CVE-2026-73722	7.2 HIGH
> CVE-2026-73723	7.1 HIGH
> CVE-2026-73724	7.1 HIGH

> CVE-2026-73725	7.0 HIGH
> CVE-2026-73726	6.8 MEDIUM
> CVE-2026-73727	6.5 MEDIUM
> CVE-2026-73728	6.5 MEDIUM
> CVE-2026-73729	6.5 MEDIUM
> CVE-2026-73731	6.1 MEDIUM
> CVE-2026-73732	5.6 MEDIUM
> CVE-2026-73733	5.4 MEDIUM
> CVE-2026-73734	5.4 MEDIUM
> CVE-2026-73735	5.4 MEDIUM
> CVE-2026-73736	5.3 MEDIUM
> CVE-2026-73737	4.8 MEDIUM
> CVE-2026-73739	4.4 MEDIUM
> CVE-2026-73740	4.4 MEDIUM
> CVE-2026-73741	4.3 MEDIUM
> CVE-2026-73742	4.3 MEDIUM
> CVE-2026-73744	3.5 LOW
> CVE-2026-73745	3.1 LOW
> CVE-2026-73746	3.1 LOW
> CVE-2026-73747	2.5 LOW

CWE's

CWE	Beschrijving
➤ CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
➤ CWE-73	External Control of File Name or Path
➤ CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
➤ CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
➤ CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
➤ CWE-94	Improper Control of Generation of Code ('Code Injection')
➤ CWE-290	Authentication Bypass by Spoofing
➤ CWE-306	Missing Authentication for Critical Function
➤ CWE-352	Cross-Site Request Forgery (CSRF)
➤ CWE-552	Files or Directories Accessible to External Parties
➤ CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
➤ CWE-863	Incorrect Authorization

Getroffen producten

Aruba Networks
Fabric Composer
Hewlett Packard Enterprise (HPE)
Fabric Composer

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.