



Advisory NCSC-2026-0432

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in HPE Brocade Fabric OS

Publicatiedatum: 16-10-2026

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 delen. 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

HPE heeft meerdere beveiligingsproblemen verholpen in Brocade Fabric OS, specifiek in versies vóór 10.0.1 en in de 9.2.x en 10.0.x release lijnen.

Duiding

De kwetsbaarheden omvatten onder andere authenticatieomzeiling, denial of service, informatielekken, privilege-escalatie, buffer overflows, command injection, en arbitrary code execution. Aanvallers kunnen via verschillende aanvalsvectoren, zoals speciaal vervaardigde managementverzoeken, REST API-aanroepen, web management interfaces, en configuratiebestanden, ongeautoriseerde administratieve acties uitvoeren, root-commando's lokaal of op andere fabric-leden uitvoeren, en systeempromessen laten crashen.

Sommige kwetsbaarheden maken het mogelijk om sessiecontext te vervalsen, HTTP-headers te spoofen, en gevoelige systeem- en monitoringdata in te zien zonder juiste rechten. Daarnaast zijn er race conditions en thread-safety problemen die leiden tot onjuiste toegangscontrole en audit logging. Specifieke componenten zoals de diagnostic kernel module, IKEv2 protocol handler, WebTools interface, en REST API zijn betrokken bij deze kwetsbaarheden.

Sommige problemen vereisen geauthenticeerde toegang, terwijl andere ook door niet-geauthenticeerde, netwerknabije aanvallers kunnen worden misbruikt. De kwetsbaarheden beïnvloeden de integriteit, vertrouwelijkheid en beschikbaarheid van de fabric operating system omgeving en de onderliggende netwerk- en opslaginfrastructuur.

Oplossingen

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

Referenties

- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39072>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39073>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39082>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39131>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39134>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39135>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39136>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39137>

- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39138>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39139>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39140>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39141>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39142>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39143>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39144>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39145>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39146>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39147>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39148>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39149>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39150>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39151>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39152>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39153>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39154>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39155>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39156>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39157>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39158>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39159>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39160>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39161>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39163>
- <https://support.broadcom.com/external/content/SecurityAdvisories/0/39164>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-87659	7.1 HIGH
CVE-2026-87660	7.0 HIGH
CVE-2026-87661	6.8 MEDIUM
CVE-2026-87663	7.1 HIGH
CVE-2026-87664	8.5 HIGH
CVE-2026-87665	6.0 MEDIUM
CVE-2026-87666	8.6 HIGH
CVE-2026-87667	8.4 HIGH
CVE-2026-87668	6.9 MEDIUM
CVE-2026-87669	5.1 MEDIUM
CVE-2026-87670	5.1 MEDIUM
CVE-2026-87671	7.1 HIGH
CVE-2026-87672	6.8 MEDIUM
CVE-2026-87673	7.0 HIGH
CVE-2026-87674	8.5 HIGH
CVE-2026-87675	7.3 HIGH
CVE-2026-87676	6.9 MEDIUM
CVE-2026-87677	5.4 MEDIUM
CVE-2026-87678	6.9 MEDIUM
CVE-2026-87679	8.5 HIGH
CVE-2026-87688	8.5 HIGH
CVE-2026-94575	6.9 MEDIUM
CVE-2026-94576	5.9 MEDIUM
CVE-2026-94577	7.3 HIGH
CVE-2026-94578	7.5 HIGH
CVE-2026-94579	5.4 MEDIUM
CVE-2026-94580	5.7 MEDIUM
CVE-2026-94581	8.5 HIGH

CVE	CVSS Score
CVE-2026-94582	6.8 MEDIUM
CVE-2026-94583	2.1 LOW
CVE-2026-94584	2.1 LOW
CVE-2026-94585	7.7 HIGH
CVE-2026-94586	8.5 HIGH
CVE-2026-94587	6.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-15	External Control of System or Configuration Setting
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
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-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
CWE-93	Improper Neutralization of CRLF Sequences ('CRLF Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-187	Partial String Comparison
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-290	Authentication Bypass by Spoofing
CWE-306	Missing Authentication for Critical Function
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-483	Incorrect Block Delimitation

CWE	Beschrijving
CWE-532	Insertion of Sensitive Information into Log File
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-862	Missing Authorization

Getroffen producten

Broadcom

Fabric OS

HPE

Brocade Fabric OS

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 or 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.