



Advisory NCSC-2026-0413 revisie 1.0.1

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in HPE Networking AOS-Switch

Publicatiedatum: 12-10-2026

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.

Update Revisie

Per abuis is CVE-2026-76743 in de advisory vermeld zonder het jaartal 2026. Dit is inmiddels gecorrigeerd.

Feiten

HPE Networking, onder andere bekend als HPE Aruba Networking, heeft meerdere kwetsbaarheden verholpen in de HPE Networking AOS-Switch (AOS-S).

Duiding

De kwetsbaarheden bevinden zich onder andere in de management interface en API van AOS-S. 6 van de verholpen kwetsbaarheden hebben een CVSS-score van 9 tot 9.8.

De kwetsbaarheden met kenmerk CVE-2026-76742 en CVE-2026-76743 hebben een CVSS-score van 9.8. De kwetsbaarheden bevinden zich in de managementinterface van AOS-S en maken het mogelijk voor een niet-geauthenticeerde externe aanvaller om authenticatiecontroles te omzeilen en toegang te verkrijgen tot het systeem. Voor CVE-2026-76743 geldt dat deze alleen te misbruiken is onder door HPE niet gespecificeerde randvoorwaarden.

De kwetsbaarheid met kenmerk CVE-2026-76744 heeft een CVSS-score van 9.8. Het betreft een buffer overflow die door een niet-geauthenticeerde externe aavaller misbruikt kan worden om willekeurige code uit te voeren op het getroffen systeem.

De kwetsbaarheid met kenmerk CVE-2026-76745 heeft een CVSS-score van 9.6. Wanneer een ongeauthenticeerde aanvaller vanuit een aangrenzend netwerk deze fout misbruikt kan dit leiden tot geheugen corruptie en het uitvoeren van willekeurige code op het getroffen systeem.

De kwetsbaarheid met kenmerk CVE-2026-76746 heeft een CVSS-score van 9.3. Het betreft een buffer overflow die door een niet-geauthenticeerde aanvaller vanuit een aangrenzend netwerk misbruikt kan worden en kan leiden tot het lekken van gevoelige informatie of het veroorzaken van een denial of service op het getroffen systeem.

De kwetsbaarheid met kenmerk CVE-2026-76747 heeft een CVSS-score van 9.1. Het betreft een buffer overflow die door een niet-geauthenticeerde externe aanvaller misbruikt kan worden. Misbruik van deze fout kan leiden tot het lekken van gevoelige informatie of denial of service op het getroffen systeem.

De succesvolle exploitatie van deze kwetsbaarheden kan de vertrouwelijkheid, integriteit en beschikbaarheid van het getroffen systeem beïnvloeden.

Oplossingen

Het NCSC adviseert om managementinterfaces niet aan het internet te koppelen, maar enkel op aparte managementnetwerken beschikbaar te stellen. Dit beperkt het aanvalsoppervlak aanzienlijk. Daarnaast adviseert het NCSC om IP-allowlisting toe te passen en de AOS-S interface enkel voor vertrouwde clients beschikbaar te stellen.

HPE Networking heeft updates uitgebracht om de kwetsbaarheden in AOS-S te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05156en_us&docLocale=en_US

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-76742	9.8 CRITICAL
CVE-2026-76743	9.8 CRITICAL
CVE-2026-76744	9.8 CRITICAL
CVE-2026-76745	9.6 CRITICAL
CVE-2026-76746	9.3 CRITICAL
CVE-2026-76747	9.1 CRITICAL
CVE-2026-76748	8.8 HIGH
CVE-2026-76741	6.5 MEDIUM
CVE-2026-76749	6.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-121	Stack-based Buffer Overflow
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Getroffen producten

Hewlett Packard Enterprise (HPE)
AOS-Switch (AOS-S)

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.