



Advisory NCSC-2026-0454

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in HPE Networking AOS

Publicatiedatum: 26-10-2026

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 72 kwetsbaarheden verholpen in HPE Networking AOS-8 en AOS-10, waaronder Mobility Conductors, Mobility Controllers, Mobility Gateways en Access Points.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen, waaronder authenticatieomzeiling, command- en SQL-injectie, buffer-overflows en onvoldoende toegangscontrole. Van de in totaal 72 kwetsbaarheden zijn 33 als kritiek aangemerkt. Hiervan kunnen 19 volgens HPE Networking zonder authenticatie op afstand via het netwerk worden misbruikt. Voor de overige 14 kritieke kwetsbaarheden is volgens HPE Networking eveneens geen authenticatie vereist, maar moet de aanvaller toegang hebben tot een aangrenzend netwerk. Succesvol misbruik kan onder meer leiden tot het uitvoeren van willekeurige code, het verkrijgen van administratieve toegang, het wijzigen van configuraties, het uitlezen van gevoelige informatie en Denial-of-Service.

Van de 33 kritieke kwetsbaarheden hebben acht een CVSS-score van 10.0. De kwetsbaarheden met kenmerk CVE-2026-79844, CVE-2026-79845, CVE-2026-79846, CVE-2026-79847, CVE-2026-79848, CVE-2026-79849, CVE-2026-79850 en CVE-2026-79851 kunnen zonder authenticatie en gebruikersinteractie op afstand worden misbruikt. Zeven hiervan kunnen leiden tot het uitvoeren van willekeurige code. CVE-2026-79845 kan leiden tot het verkrijgen van administratieve toegang en het wijzigen of uitlezen van gevoelige gegevens. Voor sommige kwetsbaarheden gelden aanvullende voorwaarden. Hoewel CVE-2026-79844 en CVE-2026-79846 een CVSS-score van 10.0 hebben, vermeldt HPE dat misbruik afhankelijk kan zijn van voorwaarden buiten de controle van de aanvaller.

De kwetsbaarheden met kenmerk CVE-2026-79857 en CVE-2026-79860 in het PAPI-protocol van AOS-8, kunnen zonder authenticatie op afstand worden misbruikt door speciaal vervaardigde UDP-pakketten te versturen. Succesvol misbruik kan leiden tot het uitvoeren van willekeurige code met verhoogde rechten en mogelijk volledige compromittering van het systeem.

HPE Networking meldt niet op de hoogte te zijn van publieke exploitcode en zijn geen bevestigde gevallen van actief misbruik bekend. Het NCSC adviseert om de beveiligingsupdates voor de kritieke kwetsbaarheden met voorrang toe te passen.

Oplossingen

HPE heeft beveiligingsupdates uitgebracht om de kwetsbaarheden te verhelpen. Organisaties wordt geadviseerd te upgraden naar AOS-10.8.1.2, 10.7.2.7, 10.4.1.14, AOS-8.13.3.1 of 8.10.0.24, of latere versies binnen de betreffende ondersteunde releasebranches.

HPE adviseert daarnaast de CLI- en webmanagementinterfaces af te schermen via een afzonderlijk VLAN en/of firewallregels. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05162en_us&docLocale=en_US

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-79844	10.0 CRITICAL
CVE-2026-79845	5.5 MEDIUM
CVE-2026-79846	10.0 CRITICAL
CVE-2026-79847	10.0 CRITICAL
CVE-2026-79848	10.0 CRITICAL
CVE-2026-79849	10.0 CRITICAL
CVE-2026-79850	10.0 CRITICAL
CVE-2026-79851	10.0 CRITICAL
CVE-2026-79852	9.8 CRITICAL
CVE-2026-79853	9.8 CRITICAL
CVE-2026-79854	9.8 CRITICAL
CVE-2026-79855	9.8 CRITICAL
CVE-2026-79856	9.8 CRITICAL
CVE-2026-79857	9.8 CRITICAL
CVE-2026-79858	9.8 CRITICAL
CVE-2026-79859	9.8 CRITICAL

CVE	CVSS Score
CVE-2026-79860	9.8 CRITICAL
CVE-2026-79861	9.8 CRITICAL
CVE-2026-79862	9.6 CRITICAL
CVE-2026-79863	9.6 CRITICAL
CVE-2026-79864	9.6 CRITICAL
CVE-2026-79865	9.6 CRITICAL
CVE-2026-79866	9.6 CRITICAL
CVE-2026-79867	9.6 CRITICAL
CVE-2026-79868	9.6 CRITICAL
CVE-2026-79869	9.6 CRITICAL
CVE-2026-79870	9.6 CRITICAL
CVE-2026-79871	9.6 CRITICAL
CVE-2026-79872	9.4 CRITICAL
CVE-2026-79873	9.3 CRITICAL
CVE-2026-79874	9.3 CRITICAL
CVE-2026-79875	9.3 CRITICAL
CVE-2026-79876	9.3 CRITICAL
CVE-2026-79877	8.8 HIGH
CVE-2026-79878	8.8 HIGH
CVE-2026-79879	8.8 HIGH
CVE-2026-79880	8.7 HIGH
CVE-2026-79881	8.3 HIGH
CVE-2026-79882	8.3 HIGH
CVE-2026-79883	8.3 HIGH
CVE-2026-79884	8.2 HIGH
CVE-2026-79885	8.2 HIGH
CVE-2026-79886	8.2 HIGH
CVE-2026-79887	8.1 HIGH
CVE-2026-79888	8.1 HIGH
CVE-2026-79889	8.1 HIGH
CVE-2026-79890	8.1 HIGH

CVE	CVSS Score
CVE-2026-79891	8.1 HIGH
CVE-2026-79892	7.8 HIGH
CVE-2026-79893	7.5 HIGH
CVE-2026-79894	7.5 HIGH
CVE-2026-79895	7.5 HIGH
CVE-2026-79955	7.5 HIGH
CVE-2026-79956	7.2 HIGH
CVE-2026-95704	7.2 HIGH
CVE-2026-95705	7.2 HIGH
CVE-2026-95706	7.2 HIGH
CVE-2026-95707	7.2 HIGH
CVE-2026-95708	7.2 HIGH
CVE-2026-95709	7.2 HIGH
CVE-2026-95710	7.1 HIGH
CVE-2026-95711	7.1 HIGH
CVE-2026-95712	7.1 HIGH
CVE-2026-95713	7.0 HIGH
CVE-2026-95714	6.8 MEDIUM
CVE-2026-95715	6.8 MEDIUM
CVE-2026-95716	6.5 MEDIUM
CVE-2026-95717	5.5 MEDIUM
CVE-2026-95718	5.3 MEDIUM
CVE-2026-95719	4.9 MEDIUM
CVE-2026-95720	4.4 MEDIUM
CVE-2026-95721	3.3 LOW

CWE's

CWE	Beschrijving
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-266	Incorrect Privilege Assignment
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-306	Missing Authentication for Critical Function

Getroffen producten

Aruba

ArubaOS

Aruba Networks

Arubaos

Hewlett Packard Enterprise

ArubaOS (AOS)

Hewlett Packard Enterprise (HPE)

Unknown product

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.