Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0340

Kwetsbaarheden verholpen in Aruba Networks ArubaOS-CX

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

Aruba Networks heeft meerdere kwetsbaarheden verholpen in het AOS-CX netwerk besturingssysteem en de bijbehorende componenten, waaronder de command line interface, API endpoints en web-based management interface.

Duiding

De kwetsbaarheden in AOS-CX betreffen onder andere onbevoegde toegang via bypass van authenticatie, remote code execution door onjuiste verwerking van input zoals format strings en command injection, privilege escalatie door onjuiste toegang tot systeemfuncties, en denial-of-service door buffer overflows en stack overflows. Sommige kwetsbaarheden kunnen worden misbruikt zonder authenticatie, terwijl andere een geauthenticeerde gebruiker met lage privileges vereisen. Exploitatie kan leiden tot het uitvoeren van willekeurige code met verhoogde privileges, ongeautoriseerde configuratiewijzigingen, toegang tot gevoelige informatie, en verstoring van de beschikbaarheid van het systeem. Specifieke aanvalsvectoren omvatten onder meer het schrijven van bestanden via API endpoints, CSRF-aanvallen op de webinterface, SSRF-aanvallen, en het omzeilen van signature verificatie. De kwetsbaarheden zijn aanwezig in verschillende onderdelen van het AOS-CX platform, waaronder de daemon, API, command line interface en web management interface.

Oplossingen

Aruba Networks heeft updates uitgebracht om de kwetsbaarheden in AOS-CX te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05134en_us&docLocale=en_US

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-73749	9.8 CRITICAL
CVE-2026-73750	8.8 HIGH
CVE-2026-73751	8.8 HIGH
CVE-2026-73752	8.8 HIGH

CVE-2026-73753	8.8 HIGH
CVE-2026-73782	8.8 HIGH
CVE-2026-73780	8.3 HIGH
CVE-2026-73779	8.2 HIGH
CVE-2026-73778	8.1 HIGH
CVE-2026-73777	8.1 HIGH
CVE-2026-73776	7.9 HIGH
CVE-2026-73775	7.7 HIGH
CVE-2026-73774	7.6 HIGH
CVE-2026-73773	7.5 HIGH
CVE-2026-73770	7.3 HIGH
CVE-2026-73764	7.1 HIGH
CVE-2026-73763	7.1 HIGH
CVE-2026-73762	6.6 MEDIUM
CVE-2026-73761	6.5 MEDIUM
CVE-2026-73760	6.5 MEDIUM
CVE-2026-73758	6.5 MEDIUM
CVE-2026-73772	6.5 MEDIUM
CVE-2026-73757	6.4 MEDIUM
CVE-2026-73755	5.7 MEDIUM
CVE-2026-73754	5.3 MEDIUM
CVE-2026-73783	4.9 MEDIUM

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-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-134	Use of Externally-Controlled Format String
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-521	Weak Password Requirements
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

Aruba Networks
ArubaOS-CX
HPE
AOS-CX

Disclaimer