Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0330

Kwetsbaarheden verholpen in UniFi-producten van Ubiquiti

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 27-08-2026

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

Ubiquiti heeft kwetsbaarheden verholpen in verschillende UniFi-producten, waaronder UniFi Protect, UniFi OS, UniFi Network Application, UniFi Connect, UniFi Access Application, UniFi OS Server, UID Enterprise Agent, UniFi Connect Display Cast Pro, UniFi Enterprise Audio/Video Bridge en UniFi Talk.

Duiding

De kwetsbaarheden betreffen voornamelijk improper input validation en improper access control binnen de genoemde UniFi-producten. Door onvoldoende validatie van invoer kunnen kwaadwillenden met netwerktoegang, soms zonder verhoogde privileges en soms met verhoogde privileges, command injection uitvoeren op het hostapparaat. Dit maakt het mogelijk om willekeurige commando's uit te voeren met de rechten van het getroffen proces of de applicatie.

Daarnaast bevatten sommige UniFi OS-apparaten een kwetsbaarheid waarbij improper neutralization van CRLF-sequenties kan leiden tot het omzeilen van authenticatiemechanismen, wat ongeautoriseerde toegang tot apparaatfuncties of beheerinterfaces mogelijk maakt.

Verder is er een kwetsbaarheid met actieve debugcode in UniFi OS-apparaten die privilege-escalatie door een aanvaller met lage privileges op het netwerk mogelijk maakt.

De kwetsbaarheden stellen een aanvaller in staat om privileges te escaleren, ongeautoriseerde acties uit te voeren en controle over de getroffen systemen te verkrijgen. Exploitatie vereist netwerktoegang, waarbij sommige kwetsbaarheden ook zonder verhoogde privileges kunnen worden misbruikt.

Oplossingen

Ubiquiti heeft updates uitgebracht om de kwetsbaarheden in de verschillende UniFi-producten te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://community.ui.com/releases/Security-Advisory-Bulletin-067/fc4a3488-7c43-4628-8bab-f715e96dbfc9

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-77533	9.9 CRITICAL

CVE-2026-77534	9.9 CRITICAL
CVE-2026-77535	9.1 CRITICAL
CVE-2026-77536	9.9 CRITICAL
CVE-2026-77537	10.0 CRITICAL
CVE-2026-77538	8.2 HIGH
CVE-2026-77539	9.1 CRITICAL
CVE-2026-77540	9.1 CRITICAL
CVE-2026-77541	9.1 CRITICAL
CVE-2026-77542	9.1 CRITICAL
CVE-2026-77543	9.9 CRITICAL
CVE-2026-77545	9.0 CRITICAL
CVE-2026-77546	9.9 CRITICAL
CVE-2026-77547	9.9 CRITICAL
CVE-2026-77548	9.9 CRITICAL
CVE-2026-77549	9.0 CRITICAL
CVE-2026-77550	10.0 CRITICAL
CVE-2026-77551	9.0 CRITICAL
CVE-2026-77552	9.8 CRITICAL
CVE-2026-77553	9.9 CRITICAL
CVE-2026-77554	10.0 CRITICAL
CVE-2026-77557	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-93	Improper Neutralization of CRLF Sequences ('CRLF Injection')
CWE-489	Active Debug Code

Getroffen producten

Ubiquiti Inc
Cloud Gateways
Cloud Keys
Dream Machines
Dream Routers
Dream Wall
Enterprise Firewall Core
Enterprise Fortress Gateway
Enterprise Network Attached Storage
Enterprise Network Video Recorders
Express

Express 7
Network Attached Storage
Network Video Recorders
UID Enterprise Agent
UniFi Access Application
UniFi Connect Application
UniFi Enterprise Audio/ Video Bridge
UniFi OS Server
UniFi Protect AI Key
UniFi Talk Application

Disclaimer