Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0221

Kwetsbaarheden verholpen in UniFi-producten van Ubiquiti Networks

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 07-07-2026

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 Networks heeft kwetsbaarheden verholpen in verschillende UniFi-producten, waaronder UniFi Connect Application, UniFi Talk Application, UniFi Access Application, UniFi OS, UniFi Network Application en UniFi Protect Application.

Duiding

De kwetsbaarheden betreffen meerdere UniFi-producten en omvatten command injection, SQL-injectie, improper input validation, improper access control, server-side request forgery (SSRF), path traversal, authenticatie-bypass en persistent privilege escalation. Aanvallers met netwerktoegang, soms met beperkte privileges en soms na authenticatie, kunnen hierdoor onder meer willekeurige commando's uitvoeren, privileges escaleren, bestanden lezen of wijzigen, authenticatie omzeilen, en Denial of Service (DoS) veroorzaken. Sommige kwetsbaarheden vereisen gebruikersinteractie, zoals het bezoeken van een kwaadaardige website, terwijl andere direct via netwerktoegang kunnen worden misbruikt. De kwetsbaarheden zijn aanwezig in applicaties en platformen die gebruikt worden voor netwerkbeheer, toegangscontrole, video surveillance en beveiligingsmonitoring binnen de UniFi-productlijn.

Oplossingen

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

Referenties

- https://community.ui.com/releases/Security-Advisory-Bulletin-066-066/984eceb3-49c8-4227-942d-671c289b3afc

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-50746	10.0 CRITICAL
CVE-2026-50747	9.9 CRITICAL
CVE-2026-50748	9.9 CRITICAL
CVE-2026-54400	9.1 CRITICAL

CVE-2026-54401	7.7 HIGH
CVE-2026-54402	9.9 CRITICAL
CVE-2026-54403	8.6 HIGH
CVE-2026-54404	8.8 HIGH
CVE-2026-54405	7.5 HIGH
CVE-2026-54406	8.7 HIGH
CVE-2026-54407	8.6 HIGH
CVE-2026-54408	8.6 HIGH
CVE-2026-54409	7.5 HIGH
CVE-2026-55110	7.5 HIGH
CVE-2026-55111	7.5 HIGH
CVE-2026-55112	7.5 HIGH
CVE-2026-55113	7.5 HIGH
CVE-2026-55114	8.8 HIGH
CVE-2026-55115	9.9 CRITICAL
CVE-2026-55116	9.0 CRITICAL
CVE-2026-55117	8.6 HIGH
CVE-2026-55118	8.3 HIGH
CVE-2026-55119	8.1 HIGH
CVE-2026-56841	8.8 HIGH
CVE-2026-56842	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-284	Improper Access Control
CWE-665	Improper Initialization
CWE-863	Incorrect Authorization
CWE-918	Server-Side Request Forgery (SSRF)
CWE-942	Permissive Cross-domain Security Policy with Untrusted Domains

Getroffen producten

Ubiquiti Inc
Cloud Gateways
Cloud Keys
Dream Machines
Dream Routers
Dream Wall
Enterprise Firewall Core
Enterprise Fortress Gateway

Enterprise Video Recorders
Express 7
Network Attached Storage
Network Video Recorders
UniFi Access Application
UniFi Connect Application
UniFi OS Server
UniFi Protect Floodlight
UniFi Talk Application

Disclaimer