Ubiquiti UniFi Devices Use of AES-CBC Allows Key Recovery and Unauthorized Device Control

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-25651
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 22:16:19 UTC
Updated	2026-03-30 13:26:07 UTC
Description	Ubiquiti UniFi Network Controller prior to 5.10.12 (excluding 5.6.42), UAP FW prior to 4.0.6, UAP-AC, UAP-AC v2, and UAF

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000110000 probability, percentile 0.013280000 (date 2026-04-01)

Problem Types: CWE-327 | CWE-327 CWE-327 Use of a Broken or Risky Cryptographic Algorithm

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	8.7	HIGH	CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA
3.1	disclosure@vulncheck.com	Primary	8.3	HIGH	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	8.3	HIGH	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ubiquiti	UniFi Network Controller	affected 5.10.12 semver	Not specified
CNA	Ubiquiti	UniFi Network Controller	unaffected 5.6.42 semver	Not specified

CNA	Ubiquiti	UniFi UAP Firmware	affected 4.0.6 semver	Not specified
CNA	Ubiquiti	UniFi UAP-AC Firmware	affected 3.8.17 semver	Not specified
CNA	Ubiquiti	UniFi USW Firmware	affected 4.0.6 semver	Not specified
CNA	Ubiquiti	UniFi USG Firmware	affected 4.4.34 semver	Not specified

References

Reference	Source	Link	T
community.ui.com/releases/Security-Advisory-Bulletin-004-004/462e561b-9efd-4c2...	disclosure@vulncheck.com	community.ui.com	
www.vulncheck.com/advisories/ubiquiti-unifi-devices-use-of-aes-cbc-allows-key-r...	disclosure@vulncheck.com	www.vulncheck.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.