CYBER ADVISORY

Wednesday, June 24, 2026 **CAL-CSIC-202606-A-017**

Maximum-Severity Vulnerabilities Impacting Ubiquiti UniFi OS Devices

Improper Access Control	Path Traversal	Improper Input Validation	Patches Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a trio of maximum-severity vulnerabilities impacting Ubiquiti's UniFI OS devices. CVE-2026-34908, CVE-2026-34909, and CVE-2026-34910 all carry a CVSS 3.1 score of 10.0.[1] [2] [3]

CVE-2026-34908 is an Improper Access Control vulnerability that would allow an attacker who can reach the devices over the network, the ability to change system configurations. Additionally, it also enables modification of device settings that govern network operations. Successful exploitation allows the attacker to compromise the integrity of the device configuration and impacting the network services it supports. The attacker only needs network access to the target device. No credentials or privileged access are required.[4]

CVE-2026-34909 is a Path Traversal vulnerability that enables an attacker to read and manipulate files on the underlying host system in order to gain access to an underlying system account. Successful exploitation exposes the targeted device to full control and further exploitation. This vulnerability can be carried out from a host on the same network or directly connected to the target device with no authentication.[5]

CVE-2026-34910 is an Improper Input Validation vulnerability that enables an attacker with network access to supply crafted data to a UniFI OS device to execute arbitrary OS commands with device privileges. Successful exploitation of CVE-2026-34910 compromises device integrity and confidentiality. The vulnerability can be remotely executed as long as the attacker has network access to deliver the crafted inputs.[6]

Individually, successful exploitation of these vulnerabilities directly impacts an organization's confidentiality, integrity, and availability of the target organization. The vendor published a security advisory on 21 May 2026.[7] A public Proof-of-Concept and Detection was published soon after, and current open-source reporting is observing mass-exploitation of these vulnerabilities.[8]

The Cal-CSIC recommends following the vendor's guidance for patching these three vulnerabilities. To review the vendor's security advisory, please use this link:

https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b

Affected Product(s) and Version(s)

CVE	Product
CVE-2026-34908	UCG-Industrial (Version 5.0.13 and earlier) UDM, UDM-Pro, UDM-SE, UDM-Pro-Max, EFG, UDW, UDR, UDR7, Express 7, UNVR, UNVR-Pro, UNVR-Instant, ENVR, UCG-Ultra, UCG-Max and UCG-Fiber (Version 5.0.16 and earlier) UDR-5G, ENVR-Core, UCKP, UCK and UCK-Enterprise (Version 5.0.17 and earlier) UniFi OS Server (Version 5.0.6 and earlier) UNVR-G2 and UNVR-G2-Pro (Version 5.1.11 and earlier) UDM-Beast, UNAS-2, UNAS-4, UNAS-Pro, UNAS-Pro-4 and UNAS-Pro-8 (Version 5.1.8 and earlier)
CVE-2026-34909	UCG-Industrial (Version 5.0.13 and earlier) UDM, UDM-Pro, UDM-SE, UDM-Pro-Max, EFG, UDW, UDR, UDR7, Express 7, UNVR, UNVR-Pro, UNVR-Instant, ENVR, UCG-Ultra, UCG-Max and UCG-Fiber (Version 5.0.16 and earlier) UDR-5G, ENVR-Core, UCKP, UCK and UCK-Enterprise (Version 5.0.17 and earlier) UniFi OS Server (Version 5.0.6 and earlier) UNVR-G2 and UNVR-G2-Pro (Version 5.1.11 and earlier) UDM-Beast, UNAS-2, UNAS-4, UNAS-Pro, UNAS-Pro-4 and UNAS-Pro-8 (Version 5.1.8 and earlier) Express (Version 4.0.13 and earlier)
CVE-2026-34910	UCG-Industrial (Version 5.0.13 and earlier) UDM, UDM-Pro, UDM-SE, UDM-Pro-Max, EFG, UDW, UDR, UDR7, Express 7, UNVR, UNVR-Pro, UNVR-Instant, ENVR, UCG-Ultra, UCG-Max and UCG-Fiber (Version 5.0.16 and earlier) UDR-5G, ENVR-Core, UCKP, UCK and UCK-Enterprise (Version 5.0.17 and earlier) UniFi OS Server (Version 5.0.6 and earlier) UNVR-G2 and UNVR-G2-Pro (Version 5.1.11 and earlier) UDM-Beast, UNAS-2, UNAS-4, UNAS-Pro, UNAS-Pro-4 and UNAS-Pro-8 (Version 5.1.8 and earlier)

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] NVD; "CVE-2026-34908 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-34908; accessed 24 June 2026
[2] NVD; CVE-2026-34909 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-34909; accessed 24 June 2026
[3] NVD; "CVE-2026-34910 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-34910; accessed 24 June 2026
[4] OpenCVE; CVE-2026-34908"; https://app.opencve.io/cve/CVE-2026-34908; accessed 24 June 2026
[5] OpenCVE; CVE-2026-34909"; https://app.opencve.io/cve/CVE-2026-34909; accessed 24 June 2026
[6] OpenCVE; "CVE-2026-34910"; https://app.opencve.io/cve/CVE-2026-34910; accessed 24 June 2026
[7] UniFi; "Security Advisory Bulletin 064"; https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b; accessed 24 June 2026
[8] PwnDefend; " Theat Intel"; https://www.pwndefend.com/2026/06/09/cve-2026-34910-exploitation-itw-building-a-botnet-mirai/; accessed 24 June 2026