CYBER ADVISORY

Thursday, July 09, 2026 **CAL-CSIC-202607-A-005**

Multiple Critically-rated Vulnerabilities Involving A Wide Range of Ubiquiti UniFi Products

Privilege Escalation	Data Exfiltration and Persistence	CIA Compromise	Mitigations Available

The Cybersecurity Integration Center (CSIC) has become aware of several critically rated vulnerabilities involving a wide range of Ubiquiti UniFi Products. The vulnerabilities mentioned in this advisory range from a CVSS 3.1 score of 9.0 to the maximum-severity score of 10.0

CVE-2026-50746 is a maximum-severity Improper Access Control vulnerability that affects the UniFi Connect application. It enables an attacker with network access to craft and inject arbitrary shell commands. Successful exploitation gives the attacker host-level privileges to enable code execution, data exfiltration, and persistence without user interaction.[1]

CVE-2026-50747 is a critically-rated SQL injection vulnerability that is found in the UniFi Talk Application. It carries a CVSS 3.1 score of 9.9. the vulnerability allows an attacker with network access and low-privileged credentials to craft malicious SQL statements that can be used to elevate privileges on the host device. Successful exploitation of this vulnerability will give the attacker broader control of the target system and its network environment.[2]

CVE-2026-50748 is a critically-rated Improper Input Validation vulnerability that affects the UniFI Access Application and carries a CVSS 3.1 score of 9.9. It enables an attacker with network access and low privileges to inject crafted inputs to the application that can result in command injection on the host device. Successful exploitation allows the attacker to potentially execute arbitrary system commands under the privileges of the UniFi Access service – leading to device compromise and the reconfiguration or disclosure of sensitive data.[3]

CVE-2026-55115 is a critically-rated Server-Side Request Forgery vulnerability within the UniFi Protect Application that carries a CVSS 3.1 score of 9.9. It enables a low-privileged attacker that can reach over the network to make arbitrary HTTP requests to internal endpoints. Successful exploitation would allow the attacker to elevate their privileges and escalate their access level on the host device.[4]

CVE-2026-54402 is another critically-rated Improper Input vulnerability that is found in UniFi OS and also carries a CVSS 3.1score of 9.9. It allows an attacker with low-privileges and network access to send crafted input and execute arbitrary system commands on the host device. Successful exploitation would allow the attacker to run malicious commands on the device to impact the confidentiality, integrity, and availability of the targeted device and its services.[5]

CVE-2026-54400 is a critically-rated Improper Access Control vulnerability found within the UniFi Access Application and carries a CVSS 3.1 score of 9.1. It allows the attacker with network access and high local privileges to bypass the application's authorization checks to elevate privileges within the host device. Successful exploitation allows the attacker to perform unauthorized actions with the elevated privileges and potential full compromise of the host device.[6]

CVE-2026-55116 is an Improper Access Control vulnerability within UniFi OS devices and carries a CVSS 3.1 score of 9.0. If certain conditions are met, it enables an attacker with network access to modify device configurations without proper authentication. Successful exploitation allows the attacker to alter network behavior, disable services, and misconfigure routing to execute denial of service (DoS) or facilitate data exfiltration.[7]

Ubiquiti has acknowledged these vulnerabilities and has issued a security advisory bulletin with update and mitigation instructions. There is currently no evidence that these vulnerabilities are being exploited in the wild. Please note that these seven vulnerabilities are the critical vulnerabilities in their bulletin, wherein Ubiquiti has listed 25 in total.[8]

The Cal-CSIC recommends following Ubiquiti's update and mitigation guidance as soon as possible. For additional vulnerability details, please use this link:

Ubiquiti UniFI Security Bulletin:

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

Affected Product and Version

	Product	Affected Version	Fixed Version
CVE-2026-50746	UniFI Connect Application	Version 3.4.16 and earlier	Version 3.4.20 or later
CVE-2026-50747	UniFi Talk Application	Version 5.1.2 and earlier	Version 5.2.2 or later
CVE-2026-50748 CVE-2026-54400	Unifi Access Application	Version 4.2.28 and earlier	Version 4.2.29 or later
CVE-2026-55115	UniFi Protect Application	Version 7.1.77 and earlier	Version 7.1.83 or later
CVE-2026-54402	UniFi OS Server, UDM, UDM-Pro, UDM-SE, UDM-Pro-Max, UDM-Beast, EFG, UDW, UDR, UDR7, UDR-5G, Express 7, UCK, UCKP, UCK-Enterprise, UNVR, UNVR-Pro, UNVR-Instant, ENVR, ENVR-Core, UNVR-G2, UNVR-G2-Pro, UCG-Ultra, UCG-Max, UCG-Industrial and UCG-Fiber	Version 5.1.15 or earlier	Version 5.1.19 or later
	UNAS-2, UNAS-4, UNAS-Pro, UNAS-Pro-4 and UNAS-Pro-8	Version 5.1.16 or earlier	Version 5.1.19 or later
	EF-Core	Version 5.1.18 and earlier	Version 5.1.19 or later
CVE-2026-55116	UDM, UDM-Beast, UDM-Pro, UDM-SE, UDM-Pro-Max, EFG, UDW, UDR, UDR7, UDR-5G, Express 7, UCG-Ultra, UCG-Max, UCG-Industrial and UCG-Fiber	Version 5.1.15 and earlier	Version 5.1.19 or later
	EF-Core	Version 5.1.18 and earlier	Version 5.1.19 or later

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] OpenCVE; "CVE-2026-50746"; https://app.opencve.io/cve/CVE-2026-50746; accessed 09 July 2026
[2] OpenCVE; "CVE-2026-50747"; https://app.opencve.io/cve/CVE-2026-50747; accessed 09 July 2026
[3] OpenCVE; "CVE-2026-50748"; https://app.opencve.io/cve/CVE-2026-50748; accessed 09 July 2026
[4] OpenCVE; "CVE-2026-55115"; https://app.opencve.io/cve/CVE-2026-55115; accessed 09 July 2026
[5] OpenCVE; "CVE-2026-54402"; https://app.opencve.io/cve/CVE-2026-54402; accessed 09 July 2026
[6] OpenCVE; "CVE-2026-54400"; https://app.opencve.io/cve/CVE-2026-54400; accessed 09 July 2026
[7] OpenCVE; "CVE-2026-55116"; https://app.opencve.io/cve/CVE-2026-55116; accessed 09 July 2026
[8] UniFi; "Security Advisory Bulletin 066"; https://community.ui.com/releases/Security-Advisory-Bulletin-066-066/984eceb3-49c8-4227-942d-671c289b3afc; accessed 09 July 2026