An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2605220212

NCSC Advisory

Critical and High vulnerabilities: Ubiquiti: UniFi Network Application

CVE-2026-22557, CVE-2026-22558, CVE-2026-22559

22nd, May 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-22557 (**CVSS Score**[1]**:** 10), CVE-2026-22558 (**CVSS Score:** 7.7), CVE-2026-22559 (**CVSS Score:** 8.8)

Published: 2026-03-19

Vendor: Ubiquiti Inc

Product: UniFi Network Application

Products Affected

CVE	Product	Version
CVE-2026-22557 CVE-2026-22558	UniFi Express	< 4.0.13
CVE-2026-22557 CVE-2026-22558 CVE-2026-22559	UniFi Network Application	< 10.1.89
CVE-2026-22557 CVE-2026-22558	UniFi Network Application	< 10.2.97
CVE-2026-22557 CVE-2026-22558	UniFi Network Application	< 9.0.118

Impact

These vulnerabilities were first published in March 2026. Since then it has been discovered that they can be chained resulting in full network compromise: an attacker exploiting the path traversal could gain system access and then leverage the NoSQL Injection to escalate privileges, amplifying impact across the network. Exploitation would have a high impact on confidentiality, integrity, and availability.

[1] https://www.first.org/cvss/

CVE-2026-22557

A malicious actor with access to the network could exploit a Path Traversal vulnerability found in the UniFi Network Application to access files on the underlying system that could be manipulated to access an underlying account.,

Common Weakness Enumeration (CWE)[2]: CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

CVE-2026-22558

Authenticated NoSQL Injection allows a malicious actor with authenticated access to escalate privileges within the UniFi Network Application.

Common Weakness Enumeration (CWE): CWE-943: Improper Neutralization of Special Elements in Data Query Logic

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

CVE-2026-22559

An Improper Input Validation vulnerability in UniFi Network Server may allow unauthorized access to an account if the account owner is socially engineered into clicking a malicious link.

Common Weakness Enumeration (CWE): CWE-20: Improper Input Validation

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Ubiquiti Inc.

- https://nvd.nist.gov/vuln/detail/CVE-2026-22557
- https://nvd.nist.gov/vuln/detail/CVE-2026-22559
- https://nvd.nist.gov/vuln/detail/CVE-2026-22558
- https://community.ui.com/releases/Security-Advisory-Bulletin-062-062/c29719c0-405e-4d4a-8f26-e343e99f931b
- https://www.unihosted.com/blog/Ubiquiti-Security-Advisory-Bulletin-062