An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2605220207

# NCSC Advisory

## Critical Vulnerability exists in Fortinet FortiAuthenticator

CVE-2026-44277

**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 Traffc Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.**

# Description

**CVE ID:** CVE-2026-44277

**Published:** 2026-05-12

**Vendor:** Fortinet

**Product:** FortiAuthenticator

**CVSS Score[1]:** 9.1

# Products Affected

| Product | Version |
|---|---|
| FortiAuthenticator | 8.0.2 |
| FortiAuthenticator | 8.0.0 |
| FortiAuthenticator | 6.6.0 <= 6.6.8 |
| FortiAuthenticator | 6.5.0 <= 6.5.6 |
| FortiAuthenticator | 6.4.0 <= 6.4.10 |

# Impact

An Improper access control vulnerability exists in in FortiAuthenticator which may allow an unauthenticated attacker to execute unauthorized code or commands via crafted requests.

FortiAuthenticator Cloud is not impacted by this vulnerability.

Common Weakness Enumeration (CWE)[2]: CWE-284: Improper Access Control

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

Used by Ransomware Operators: N/A

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

- https://nvd.nist.gov/vuln/detail/CVE-2026-44277
- https://www.cve.org/CVERecord?id=CVE-2026-44277
- https://fortiguard.fortinet.com/psirt/FG-IR-26-128