An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2505290126

NCSC Advisory

Critical Vulnerability found in Fortinet: FortiOS, FortiProxy, FortiSwitchManager

CVE-2025-22252

29th, May 2025

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-2025-22252

Published: 2025-05-28

Vendor: Fortinet

Product: FortiOS, FortiProxy, FortiSwitchManager

CVSS Score[1]: 9.0

Products Affected

Product	Version
FortiProxy	7.6.0 <= 7.6.1
FortiSwitchManager	7.2.5
FortiOS	7.6.0
FortiOS	7.4.4 <= 7.4.6

Impact

A missing authentication for critical function in Fortinet FortiProxy versions 7.6.0 through 7.6.1, FortiSwitchManager version 7.2.5, and FortiOS versions 7.4.4 through 7.4.6 and version 7.6.0 (with TACACS+ configured to use a remote TACACS+ server for authentication, that has itself been configured to use ASCII authentication), may allow an attacker with knowledge of an existing admin account to access the device as a valid admin via an authentication bypass.

Common Weakness Enumeration (CWE)[2]: CWE-306: Escalation of privilege

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-2025-22252
- https://www.cve.org/CVERecord?id=CVE-2025-22252
- https://fortiguard.fortinet.com/psirt/FG-IR-24-472