An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2504100179

NCSC Advisory

Critical Fortinet FortiSwitch Vulnerability

CVE-2024-48887

10th, April 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-2024-48887

Published: 2025-04-08

Vendor: Fortinet

Product: FortiSwitch

CVSS Score[1]: 9.8

Products Affected

Product	Version
FortiSwitch	7.6.0
FortiSwitch	7.4.0 <= 7.4.4
FortiSwitch	7.2.0 <= 7.2.8
FortiSwitch	7.0.0 <= 7.0.10
FortiSwitch	6.4.0 <= 6.4.14

Impact

An unverified password change vulnerability in FortiSwitch GUI may allow a remote unauthenticated attacker to modify admin passwords via a specially crafted request.

Common Weakness Enumeration (CWE)[2]: CWE-620: Unverified Password Change

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

Workaround

Disable HTTP/HTTPS Access from administrative interfaces.

Configure trusted hosts to limit the hosts that can connect to the system using CLI:

config system admin

edit <admin_name>

set {trusthost1 | trusthost2 | trusthost3 | trusthost4 |

trusthost5 | trusthost6 | trusthost7 | trusthost8 | trusthost9

| trusthost10} <address_ipv4mask>

next

end

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-2024-48887
- https://www.cve.org/CVERecord?id=CVE-2024-48887
- https://fortiguard.fortinet.com/psirt/FG-IR-24-435
- https://socradar.io/fortinet-cve-2024-48887-fortiswitch-admin-credentials/