An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC 2501140211

NCSC Advisory

Critical Vulnerability in Fortinet affecting FortiOS and FortiProxy (CVE-2024-55591)

15th, January 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.

Revision History

Revision	Date	Author(s)	Description
1.0	14th January 2025	CSIRT-IE	Intial Advisory
1.1	15th January 2025	CSIRT-IE	Added to KEV, and reports of exploitation in the wild

Description

CVE ID: CVE-2024-55591

Published: 2025-01-14

Vendor: Fortinet

Product: FortiProxy, FortiOS

CVSS Score[1]: 9.6

Products affected

Product	Version
FortiOS	7.0.0 <= 7.0.16
FortiProxy	7.2.0 <= 7.2.12
FortiProxy	7.0.0 <= 7.0.19

Impact

An authentication bypass using an alternate path or channel vulnerability [CWE-288] affecting FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12 allows a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module.
Please note that reports show this is being exploited in the wild.

[1] https://www.first.org/cvss/v3.0/specification-document

Common Weakness Enumeration (CWE)[2]**:** CWE-288: Execute unauthorized code or commands

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

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, examine their systems for indicators of compromise within the below articles and install the relevant updates from Fortinet.

- https://nvd.nist.gov/vuln/detail/CVE-2024-55591
- https://www.cve.org/CVERecord?id=CVE-2024-55591
- https://fortiguard.fortinet.com/psirt/FG-IR-24-535

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog