An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2505140007

NCSC Advisory

Critical Vulnerability found in Fortinet: FortiNDR, FortiRecorder, FortiVoice, FortiMail, FortiCamera

14th, 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-2025-32756

Published: 2025-05-13

Vendor: Fortinet

Product: FortiNDR, FortiRecorder, FortiVoice, FortiMail, FortiCamera

CVSS Score[1]**:** 9.6

Products Affected

Product	Version
FortiVoice	7.2.0 7.0.0 <= 7.0.6 6.4.0 <= 6.4.10
FortiRecorder	7.2.0 <= 7.2.3 7.0.0 <= 7.0.5 6.4.0 <= 6.4.5
FortiMail	7.6.0 <= 7.6.2 7.4.0 <= 7.4.4 7.2.0 <= 7.2.7 7.0.0 <= 7.0.8
FortiNDR	7.6.0 7.4.0 <= 7.4.7 7.2.0 <= 7.2.4 7.1.0 <= 7.1.1 7.0.0 <= 7.0.6 1.5.0 <= 1.5.3 1.4.0 1.3.0 <= 1.3.1 1.2.0 1.1.0

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

Impact

A stack-based overflow vulnerability [CWE-121] in FortiVoice, FortiMail, FortiNDR, FortiRecorder and FortiCamera may allow a remote unauthenticated attacker to execute arbitrary code or commands via crafted HTTP requests. Fortinet has observed this to be exploited in the wild on FortiVoice.

The operations performed by the Threat Actor in the case observed were part or all of the below:

- Scan the device network
- Erase system crashlogs
- Enable fcgi debugging to log credentials from the system or SSH login attempts

Common Weakness Enumeration (CWE)[2]: CWE-121: Execute unauthorized code or commands

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

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 and install the relevant updates from Fortinet.

- https://nvd.nist.gov/vuln/detail/CVE-2025-32756
- https://www.cve.org/CVERecord?id=CVE-2025-32756
- https://fortiguard.fortinet.com/psirt/FG-IR-25-254

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

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