National Cyber Security Centre

2402120137-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerabilities in Fortinet FortiOS (CVE-2024-21762, CVE-2024-23113)

UPDATE

Friday 18th October, 2024

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	9th February 2024	CSIRT-IE	Initial advisory responding to Fortinet advisory
1.1	12th February 2024	CSIRT-IE	Update with details of additional affected FortiOS operating systems for CVE-2024-21762 and CVE-2024-23113.
1.2	20th March 2024	CSIRT-IE	Update with details of a public POC release and active exploitation for CVE-2024-21762.
1.3	18th October 2024	CSIRT-IE	Update with additional products affected for CVE-2024-23113.

Description

Published: Feb 9th 2024
Vendor: Fortinet
Product: FortiOS

CVE ID: CVE-2024-21762
CVSS3.0 Score[1]**:** 9.8
EPSS[2]**:** 0.893990000

CVE ID: CVE-2024-23113
CVSS3.0 Score: 9.8
EPSS: 0.376120000

Summary: Fortinet has disclosed two critical vulnerabilities affecting its FortiOS operating system.

CVE-2024-21762 is due to incorrect parameter checks in FortiOS SSL-VPN. It may allow a remote unauthenticated attacker to execute arbitrary code or command via specially crafted HTTP requests.

CVE-2024-23113 is due to an externally controlled format string vulnerability in FortiOS fgfmd daemon, and may allow a remote unauthenticated attacker to execute arbitrary code or commands via specially crafted requests.

More information related to these issues can be found at the following links:

- https://www.fortiguard.com/psirt/FG-IR-24-015
- https://www.fortiguard.com/psirt/FG-IR-24-029

Products Affected

CVE-2024-21762:

- FortiOS 7.4.0 - 7.4.2
- FortiOS 7.2.0 - 7.2.6
- FortiOS 7.0.0 - 7.0.13
- FortiOS 6.4.0 - 6.4.14
- FortiOS 6.2.0 - 6.2.15
- FortiOS 6.0 all versions
- FortiProxy 7.4.0 - 7.4.2
- FortiProxy 7.2.0 - 7.2.8
- FortiProxy 7.0.0 - 7.0.14
- FortiProxy 2.0.0 - 2.0.13
- FortiProxy 1.2 all versions
- FortiProxy 1.1 all versions

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

- FortiProxy 1.0 all versions

CVE-2024-23113:

- FortiOS 7.4.0 - 7.4.2
- FortiOS 7.2.0 - 7.2.6
- FortiOS 7.0.0 - 7.0.13
- FortiPAM 1.2
- FortiPAM 1.1.0 - 1.1.2
- FortiPAM 1.0 all versions
- FortiProxy 7.4.0 - 7.4.2
- FortiProxy 7.2.0 - 7.2.8
- FortiProxy 7.0.0 - 7.0.14
- FortiSwitchManager 7.2.0 - 7.2.3
- FortiSwitchManager 7.0.0 - 7.0.3
- UPDATE, 18th October: FortiSwitchManager 7.2 7.2.0 through 7.2.3 Upgrade to 7.2.4 or above
- UPDATE, 18th October: FortiSwitchManager 7.0 7.0.0 through 7.0.3 Upgrade to 7.0.4 or above

Impact

Unauthenticated attackers can use the vulnerabilities to execute arbitrary code on affected devices.

Common Weakness Enumeration (CWE)[3]: CVE-2024-21762(CWE-787), CVE-2024-23113(CWE-134)

Present in CISA Known Exploited Vulnerability(KEV)[4] catalog: Yes (CVE-2024-21762)

CVE-2024-21762: There has been an observed increase in exploitation activity following the release of a detailed public proof-of-concept (PoC) exploit.

Recommendations

CVE-2024-21762: Fortinet have given a workaround which is to disable SSL VPN on your FortiOS devices (disable webmode is NOT a valid workaround). Patches have been released for all FortiOS and FortiProxy versions except for FortiOS 6.0 and FortiProxy 1.0, 1.1 and 1.2 where the advice is to migrate to a fixed release.

CVE-2024-23113: Fortinet have provided a workaround which is to remove the fgfm access from each interface, further information on this workaround is available here: https://www.fortiguard.com/psirt/FG-IR-24-029. Patches have been released for all affected FortiOS operating systems except FortiPAM 1.0 where the advice is to migrate to a fixed release.

Please also note that a local-in policy that only allows FGFM connections from a specific IP will reduce the attack surface but it won't prevent the vulnerability from being exploited from this IP. As a consequence, this should be used as a mitigation and not as a complete workaround.

[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

The NCSC strongly advises affected organisations to review the latest Fortinet release notes and install the relevant updates using Fortinet's upgrade tool which can be found here: https://docs.fortinet.com/upgrade-tool.

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 K7X4,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre