An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2412190132

NCSC Advisory

Multiple Vulnerabilities in Fortinet Products

19th, December 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.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Description

Fortinet has identified three vulnerabilities, ranging from critical to medium severity impacting its FortiWLM, FortiManager, FortiClientLinux, and FortiClientWindows products.

Published: 2024-12-18

Vendor: Fortinet

Products Affected

Product	Version	CVE	CVSS Score
FortiWLM	8.6.0 through 8.6.5	CVE-2023-34990	9.6
FortiWLM	8.5.0 through 8.5.4	CVE-2023-34990	9.6
FortiManager 7.6	7.6.0	CVE-2024-48889	7.2
FortiManager 7.4	7.4.0 through 7.4.4	CVE-2024-48889	7.2
FortiManager 7.4	Cloud 7.4.1 through 7.4.4	CVE-2024-48889	7.2
FortiManager 7.2	7.2.3 through 7.2.7	CVE-2024-48889	7.2
FortiManager 7.2	Cloud 7.2.1 through 7.2.7	CVE-2024-48889	7.2
FortiManager 7.0	7.0.5 through 7.0.12	CVE-2024-48889	7.2
FortiManager 7.0	Cloud 7.0.1 through 7.0.12	CVE-2024-48889	7.2
FortiManager 6.4	6.4.10 through 6.4.14	CVE-2024-48889	7.2
FortiClientLinux 7.4	7.4.0 through 7.4.2	CVE-2024-50570	4.9
FortiClientLinux 7.2	7.2.0 through 7.2.7	CVE-2024-50570	4.9
FortiClientLinux 7.0	7.0.0 through 7.0.13	CVE-2024-50570	4.9
FortiClientWindows 7.4	7.4.0 through 7.4.1	CVE-2024-50570	4.9
FortiClientWindows 7.2	7.2.0 through 7.2.6	CVE-2024-50570	4.9
FortiClientWindows 7.0	7.0.0 through 7.0.13	CVE-2024-50570	4.9

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Impact

CVE-2023-34990 is a critical relative path traversal vulnerability in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 which allows an attacker to execute unauthorized code or commands via specially crafted web requests.

- **Common Weakness Enumeration (CWE):** CWE-23[1] Execute unauthorized code or commands.

CVE-2024-48889 is a high severity vulnerability for Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78[2]] in FortiManager version 7.6.0, version 7.4.4 and below, version 7.2.7 and below, version 7.0.12 and below, version 6.4.14 and below and FortiManager Cloud version 7.4.4 and below, version 7.2.7 to 7.2.1, version 7.0.12 to 7.0.1 may allow an authenticated remote attacker to execute unauthorized code via FGFM crafted requests.

- **Common Weakness Enumeration (CWE):** CWE-78 Execute Unauthorized Code or Commands; DoS: Crash, Exit, or Restart; Read Files or Directories; Modify Files or Directories; Read Application Data; Modify Application Data; Hide Activities

CVE-2024-50570 is a medium severity Cleartext Storage of Sensitive Information vulnerability [CWE-312[3]] in FortiClientWindows 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13 and FortiClientLinux 7.4.0 through 7.4.2, 7.2.0 through 7.2.7, 7.0.0 through 7.0.13 may permit a local authenticated user to retrieve VPN password via memory dump, due to JavaScript's garbage collector

- **Common Weakness Enumeration (CWE):** CWE-312 Read Application Data

None of these vulnerabilities are listed within the Known Exploited Vulnerability (KEV) catalog[4] or are known to be used by Ransomware Operators.

[1] https://cwe.mitre.org/data/definitions/23.html
[2] https://cwe.mitre.org/data/definitions/78.html
[3] https://cwe.mitre.org/data/definitions/312.html
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

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-2023-34990
- https://www.cve.org/CVERecord?id=CVE-2023-34990
- https://fortiguard.com/psirt/FG-IR-23-144
- https://nvd.nist.gov/vuln/detail/CVE-2024-48889
- https://www.cve.org/CVERecord?id=CVE-2024-48889
- https://www.fortiguard.com/psirt/FG-IR-24-425
- https://nvd.nist.gov/vuln/detail/CVE-2024-50570
- https://www.cve.org/CVERecord?id=CVE-2024-50570
- https://www.fortiguard.com/psirt/FG-IR-23-278