An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2410170128

NCSC Advisory

Critical Vulnerability in Fortinet FortiManager (CVE-2024-47575)

12 November 2024

Update 1.2

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

Revision History

Revision	Date	Author(s)	Description
1.0	24th October 2024	CSIRT-IE	Intial Advisory
1.1	1st November 2024	CSIRT-IE	Updated IP list and Serial Number
1.2	11th November 2024	CSIRT-IE	Added recommendation for managed devices

Description

CVE ID: CVE-2024-47575

Published: 2024-10-23

Vendor: FortiGuard labs

Product: FortiManager, FortiManager Cloud

CVSS3.0 Score[1]: 9.8

Summary: Fortinet is disclosing a critical vulnerability in FortiManager. A missing authentication for a critical function vulnerability [CWE-306] in FortiManager fgfmd daemon may allow a remote unauthenticated attacker with a valid Fortinet certificate extracted from a Fortinet device or VM to execute artbitrary code or commands via specially crafted requests.

FortiGuard Alert: https://www.fortiguard.com/psirt/FG-IR-24-423

Reports have shown this vulnerability to be exploited in the wild.

Products Affected & Solutions

Version	Affected	Solution
FortiManager 7.6	7.6.0	Upgrade to 7.6.1 or above
FortiManager 7.4	7.4.0 through 7.4.4	Upgrade to 7.4.5 or above
FortiManager 7.2	7.2.0 through 7.2.7	Upgrade to 7.2.8 or above
FortiManager 7.0	7.0.0 through 7.0.12	Upgrade to 7.0.13 or above
FortiManager 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiManager 6.2	6.2.0 through 6.2.12	Upgrade to 6.2.13 or above
FortiManager Cloud 7.6	Not affected	Not Applicable
FortiManager Cloud 7.4	7.4.1 through 7.4.4	Upgrade to 7.4.5 or above
FortiManager Cloud 7.2	7.2 all versions	Migrate to a fixed release
FortiManager Cloud 7.0	7.0 all versions	Migrate to a fixed release
FortiManager Cloud 6.4	6.4 all versions	Migrate to a fixed release

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

Impact

A remote attacker could use this vulnerability to may allow a remote unauthenticated attacker to execute arbitrary code or commands via specially crafted requests.

Common Weakness Enumeration (CWE)[2]: CWE-306

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

Used by Ransomware Operators: Not Known

Workarounds

Upgrade to a fixed version or use one of the following workarounds, depending on the version you're running:

1. For FortiManager versions 7.0.12 or above, 7.2.5 or above, 7.4.3 or above (but not 7.6.0), prevent unknown devices to attempt to register:

   ```
   config system global
   (global)# set fgfm-deny-unknown enable
   (global)# end
   ```

   Warning: With this setting enabled, be aware that if a FortiGate's SN is not in the device list, FortiManager will prevent it from connecting to register upon being deployed, even when a model device with PSK is matching.

2. Alternatively, for FortiManager versions 7.2.0 and above, you may add local-in policies to whitelist the IP addresses of FortiGates that are allowed to connect.

   Example:

   ```
   config system local-in-policy
   edit 1

   set action accept
   set dport 541
   set src
   next
   edit 2
   set dport 541
   next
   end
   ```

3. For 7.2.2 and above, 7.4.0 and above, 7.6.0 and above it is also possible to use a custom certificate which will mitigate the issue:

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

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

```
config system global
set fgfm-ca-cert
set fgfm-cert-exclusive enable

end
```

And install that certificate on FortiGates. Only this CA will be valid, this can act as a workaround, providing the attacker cannot obtain a certificate signed by this CA via an alternate channel.

NOTE: For FortiManager versions 6.2, 6.4, and 7.0.11 and below, please upgrade to one of the versions above and apply the above workarounds.

Indicators of Compromise

Log Entries

```
type=event,subtype=dvm,pri=information,desc="Device,manager,gene
ric,information,log",user="device,...",msg="Unregistered device
localhost add succeeded" device="localhost" adom="FortiManager"
session_id=0 operation="Add device" performed_on="localhost"
changes="Unregistered device localhost add succeeded"
```

```
type=event,subtype=dvm,pri=notice,desc="Device,Manager,dvm,log,a
t,notice,level",user="System",userfrom="",msg="" adom="root"
session_id=0 operation="Modify device" performed_on="localhost"
changes="Edited device settings (SN FMG-VMTM23017412)"
```

IP Addresses

- 45.32.41.202
- 104.238.141.143
- 158.247.199.37
- 45.32.63.2
- 80.66.196.199
- 195.85.114.78 (Not observed by Fortinet, reported by Mandiant here)
- 172.232.167.68 (Not observed by Fortinet, reported by trusted third party)

Serial Number

FMG-VMTM23017412

FMG-VMTM19008093

Files

/tmp/.tm
/var/tmp/.tm

Note that file IoCs may not appear in all cases.

Recovery Methods

FortiGuard have provided the following 2 options for recovery:

Option 1 – Recommended Recovery Action

This method ensures that the FortiManager configuration was not tampered with. It will require database rebuilding or device configuration resynchronizations at the Device and Policy Package ADOM levels.

- Installing a fresh FortiManager VM or re-initializing a hardware model and adding/discovering the devices.
- Installing a fresh FortiManager VM or re-initializing a hardware model, and restoring a backup taken before the IoC detection.

Option 2 – Alternative Recovery Action

This method provides a quick recovery, where partial or no database rebuilding/resynchronization is required. It requires that you manually verify accuracy of the currently running FortiManager configuration

- Installing a fresh FortiManager VM or re-initializing a hardware model and restoring/copying components or configuration sections from a compromised FortiManager.
- Installing a fresh FortiManager VM or re-initializing a hardware model, and restoring a backup from a compromised FortiManager.

For more info on data configuration and synchronization procedures:
https://community.fortinet.com/t5/FortiManager/Technical-Tip-FortiManager-data-configuration-and/ta-p/351748

Managed Devices

Its is recommended that credentials, such as passwords and user-sensitive data, of all managed devices be urgently changed, including those of the Managed FortiGates and FortiManager. This includes:

- Admin Users Accounts

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

- Certificate's private key and password (In case of ssl offloading/deep inspection/ipsec auth)
- VPN Pre-Shared Keys
- Local user accounts
- TACACS Key
- LDAP / Active Directory Passwords
- RADIUS Secret Keys
- SNMP Secrets
- OSPF/BGP Neighbour Passwords
- Wireless SSID / Mesh Keys
- Passwords stored inside automation stitches
- PPPoE Passwords
- SMTP Passwords
- HA Pre-shared Keys Cluster Password