ultraviolet

CONFIDENTIAL

THREAT REPORT:

Fortinet RCE Exploit, Patch Now!

Services Performed By:
UltraViolet Cyber
Casey Latham
(443) 351-7630
info@uvcyber.com

Published Date:
03/20/2024

Contents

1 Executive Summary

A proof-of-concept RCE (Remote Code Execution) exploit was co-discovered by researchers against Fortinet's FortiClient Enterprise Management Server (EMS); FortiClient EMS 7.2 (Versions 7.2.0 through 7.2.2) and FortiClient EMS 7.0 (7.0.1 through 7.0.10). This exploit will allow a bad actor to perform remote code execution through specially crafted SQL Injection strings against the victim machine. In response to this exploit, Fortinet has issues patches that should be applied to affected FortiClient EMS software packages immediately.

2 Technical Analysis

The Co-discoverers of the proof-of-concept RCE (Remote Code Execution) exploit, tracked as CVE-2023-48788, have exploited Fortinet's FortiClient Enterprise Management Server (EMS); software packages FortiClient EMS 7.2 (Versions 7.2.0 through 7.2.2) and FortiClient EMS 7.0 (7.0.1 through 7.0.10). This exploit is notable as the bad actor would be able to perform remote code execution while being unauthenticated. This adds an additional layer of exploitability, as the bad actor would not have to be authenticated to the victim machine running a vulnerable version of FortiClient EMS. The SQL Injection would then allow for Remote Code Execution on the victim machine.

A SQL Injection exploit is performed by manipulating SQL queries to perform malicious actions against a victim machine, database, or remote system. The vulnerable version of FortiClient EMS will allow these queries to be ran and according to the Co-Discoverers, will allow Remote Code Execution. This is a stringed attack because the SQL injection (affecting the SQL Query) will allow Remote Code Execution (affecting systems, databases, files).

Remote Code Execution is a vulnerability where remote code (read commands) can be ran against the victim machine. In this case, the bad actor would not even have to be authenticated, so they can “fuzz” the vulnerable system to find additional vulnerabilities that can provide elevated privileges, leverage movement, and other ways that can provide deeper access into the network.

Fortinet has released a patch that will solve this vulnerability and our team at UltraViolet Cyber

recommends that the patches be applied on vulnerable systems as soon as possible. Fortinet acknowledged the vulnerability and the Fortinet Product Security Incident Response Team (PSIRT) issued patches under: PSIRT - Pervasive SQL injection in DAS component (IR # FG-IR-24-007) on March 12, 2024.

PSIRT issues the following matrix to easily identify affected versions and patch levels:

VERSION	AFFECTED	SOLUTION
FORTICLIENT EMS 7.2	7.2.0 through 7.2.2	Upgrade to 7.2.3 or above
FORTICLIENT EMS 7.0	7.0.1 through 7.0.10	Upgrade to 7.0.11 or above

Helpful Resources:

FortiGuard Information
https://www.fortiguard.com/psirt/FG-IR-24-007

CVE Information:
https://nvd.nist.gov/vuln/detail/CVE-2023-48788

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber regularly updates our IOC database to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Monitoring network logs for traffic to known malicious sites

4 What Customers Can Do

- Apply patches to vulnerable systems identified as FortiClient EMS 7.2 (Versions 7.2.0 through 7.2.2) and FortiClient EMS 7.0 (7.0.1 through 7.0.10)
- Ensure logging of SQL activities are transmitted to UltraViolet Cyber for detection and analysis

(443) 351-7630 | info@uvcyber.com

5 References

- *FortiGuard*. (n.d.-a). FortiGuard. https://www.fortiguard.com/psirt/FG-IR-24-007
- *FortiGuard*. (n.d.-b). FortiGuard. https://www.fortiguard.com/psirt
- Gatlan, S. (2024, March 21). Exploit released for Fortinet RCE bug used in attacks, patch now. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/exploit-released-for-fortinet-rce-bug-used-in-attacks-patch-now/
- *NVD - CVE-2023-48788*. (n.d.). https://nvd.nist.gov/vuln/detail/CVE-2023-48788

(443) 351-7630 | info@uvcyber.com