FortiClient EMS Vulnerability Exploited in Connect:fun Campaign

Date: 18th April 2024 | Severity: High

Summary

An improper neutralization of special elements used in an sql command (‘sql injection’) in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, FortiClientEMS 7.0.1 through 7.0.10 allows attacker to execute unauthorized code or commands via specially crafted packets.

Attack Vectors

A cyber campaign dubbed Connect:fun targets organizations with vulnerable Fortinet FortiClient EMS systems. Exploiting CVE-2023-48788, attackers gain remote access, deploying tools like Screen Connect and Powerfun, posing significant threats globally.

The Connect:fun operators manually scan for initial access to the FortiClient EMS appliance and other networks. After scanning, the threat actor attempts to execute commands as a sequence to enable advanced configuration options and the xp_cmdshell stored procedure within the SQL server. After the changes, the threat actors attempt to execute several SQL injections with obfuscated commands to download the ScreenConnect remote management tool and a malicious script that is based on the open-source tool, Powerfun. This script is used to bind and reverse shells and execute arbitrary commands from the command and control (C&C) server.

CISA vulnerability name:
Fortinet FortiClient EMS SQL Injection Vulnerability.

Indicator of compromise

INDICATOR TYPE	INDICATORS
CVE ID	CVE-2023-48788
Domain	• jxqmwbgxygkyftpxykdk8cfkq1hy371pz.oast.fun • mci11.raow.fun
IP	• 141.136.43.188 • 95.179.241.10 • 216.245.184.86 • 185.56.83.82 • 144.202.21.16

Recommendation

Version	Affected	Solution
FortiClientEMS 7.2	7.2.0 through 7.2.2	Upgrade to 7.2.3 or above
FortiClientEMS 7.0	7.0.1 through 7.0.10	Upgrade to 7.0.11 or above

Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Reference Links

- https://www.cvedetails.com/cve/CVE-2023-48788/?q=CVE-2023-48788
- https://www.fortiguard.com/psirt/FG-IR-24-007
- https://www.hivepro.com/threat-advisory/forticlient-ems-vulnerability-exploited-in-connectfun-campaign/