مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Multiple Vulnerabilities in Fortinet FortiClientEMS and FortiManager Products

Tracking #:432315698

Date:14-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Fortinet FortiClientEMS and FortiManager products that could be exploited to gain unauthorized access on affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2023-48788 (CVSSv3 Score 9.3 Critical):** An SQL injection vulnerability in the DAS component of FortiClientEMS allows unauthenticated attackers to execute arbitrary code or commands.
- **CVE-2023-47534 (CVSSv3 Score 8.7 High):** A CSV injection vulnerability in the log download feature of FortiClientEMS enables remote unauthenticated attackers to execute commands on the administrator's workstation.
- **CVE-2023-36554 (CVSSv3 Score 7.7 High):** An improper access control vulnerability in FortiWLM MEA for FortiManager grants unauthenticated remote attackers the ability to execute arbitrary code.
- **CVE-2023-41842 (CVSSv3 Score 6.3 Medium):** A format string vulnerability in FortiManager, FortiAnalyzer, FortiAnalyzer-BigData, and FortiPortal allows privileged attackers to execute unauthorized code through crafted commands.

Affected Versions:

FortiClientEMS 7.2.0 through 7.2.2
FortiClientEMS 7.0.0 through 7.0.10
FortiClientEMS 6.4 all versions
FortiClientEMS 6.2 all versions
FortiClientEMS 6.0 all versions
FortiManager version 7.4.0 through 7.4.1
FortiManager version 7.2.0 through 7.2.3
FortiManager 7.0 all versions
FortiManager 6.4 all versions
FortiManager 6.2 all versions
FortiAnalyzer version 7.4.0 through 7.4.1
FortiAnalyzer version 7.2.0 through 7.2.3
FortiAnalyzer 7.0 all versions
FortiAnalyzer 6.4 all versions
FortiAnalyzer 6.2 all versions
FortiAnalyzer-BigData version 7.2.0 through 7.2.5
FortiAnalyzer-BigData version 7.0.1 through 7.0.6
FortiAnalyzer-BigData version 6.4.5 through 6.4.7
FortiAnalyzer-BigData version 6.2.5
FortiPortal version 6.0.0 through 6.0.14
FortiPortal 5.3 all versions

Fixed Versions:
FortiClientEMS Upgrade to 7.2.3 or above
FortiClientEMS Upgrade to 7.0.11 or above
FortiClientEMS Migrate to a fixed release
FortiClientEMS Migrate to a fixed release
FortiClientEMS Migrate to a fixed release
FortiManager version 7.4.2 or above
FortiManager version 7.2.4 or above
FortiManager version 7.0.11 or above
FortiManager version 6.4.14 or above
FortiAnalyzer version 7.4.2 or above
FortiAnalyzer version 7.2.4 or above
FortiAnalyzer version 7.0.10 or above
FortiAnalyzer-BigData version 7.4.0 or above
FortiAnalyzer-BigData version 7.2.6 or above
FortiPortal version 7.0.0 or above

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Fortinet.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://www.fortiguard.com/psirt?product=FortiManager&product=FortiClientEMS&version=