مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Security Updates-Fortinet

Tracking #:432316037

Date:10-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Fortinet released a security update to address a vulnerability in FortiOS and FortiProxy's web SSL VPN UI.

TECHNICAL DETAILS:

Fortinet has released security updates to address a vulnerability in FortiOS and FortiProxy's web SSL VPN UI that may allow a remote unauthenticated attacker to perform a Cross-Site Scripting attack via social engineering the targeted user into bookmarking a malicious samba server, then opening the bookmark.

- **CVE-2024-26006-**CVSSv3 Score,6.9 Medium- Cross site scripting vulnerability in SSL VPN web UI
- An improper neutralization of input during web page Generation vulnerability in FortiOS and FortiProxy's web SSL VPN UI

Version	Affected	Fixed Versions
FortiOS 7.4	7.4.0 through 7.4.3	Upgrade to 7.4.4 or above
FortiOS 7.2	7.2.0 through 7.2.7	Upgrade to 7.2.8 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiProxy 7.4	7.4.0 through 7.4.3	Upgrade to 7.4.4 or above
FortiProxy 7.2	7.2.0 through 7.2.9	Upgrade to 7.2.10 or above
FortiProxy 7.0	7.0.0 through 7.0.16	Upgrade to 7.0.17 or above

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating FortiOS to Fixed versions released 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://fortiguard.fortinet.com/psirt/FG-IR-23-485