مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High Severity Vulnerability in FortiSOAR

Tracking #:432316259

Date:12-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Fortinet released security updates to address a high severity vulnerability in FortiSOAR product that could enable an attacker to compromise user accounts through brute force password attacks.

TECHNICAL DETAILS:

Fortinet released security updates to address a high severity vulnerability in FortiSOAR product that could enable an attacker to compromise user accounts through brute force password attacks.

- **CVE ID:CVE-2024-4863-** An improper authorization vulnerability in FortiSOAR change password endpoint may allow an authenticated attacker to perform a brute force attack on users and administrator's password via crafted HTTP requests.
- **CVSSv3 Score 7.1 , Severity High**

Version	Affected	Solution
FortiSOAR 7.5	Not affected	Not Applicable
FortiSOAR 7.4	7.4.0 through 7.4.3	Upgrade to 7.4.4 or above
FortiSOAR 7.3	7.3.0 through 7.3.2	Upgrade to 7.3.3 or above
FortiSOAR 7.2	7.2 all versions	Migrate to a fixed release
FortiSOAR 7.0	7.0 all versions	Migrate to a fixed release

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the relevant patched version 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-24-048