مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Bypass Vulnerability in Fortinet FortiVoice

Tracking #:432315863

Date:17-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in Fortinet FortiVoice which could allow a malicious user to bypass the authentication mechanism and gain access to a vulnerable system.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE ID:** CVE-2023-40720, CVSSv3 Score 6.7
- **Severity:** Medium
- An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiVoice Enterprise may allow an authenticated attacker to read the SIP configuration of other users via crafted HTTP or HTTPS requests.

Product	Affected Version	Fixed Version
FortiVoice 7.0	7.0.0 through 7.0.1	Upgrade to 7.0.2 or above
FortiVoice 6.4	6.4.0 through 6.4.8	Upgrade to 6.4.9 or above
FortiVoice 6.0	6.0 all versions	Migrate to a fixed release

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating FortiVoice to the latest version.

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/FG-IR-23-282