مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in FortiClient Linux

Tracking #:432315760

Date:15-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Fortinet released Security updates to address a critical security vulnerability in FortiClientLinux versions.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2023-45590**
- **CVSS Score: 9.4 (Critical)**
- The vulnerability is classified as an Improper Control of Generation of Code issue (CWE-94), also known as code injection.
- **Impact**:An attacker can potentially exploit this vulnerability to trick a FortiClientLinux user into visiting a malicious website. This website can then inject malicious code that can be executed on the user's device. If successful, the attacker could gain unauthorized access to the device and potentially the entire network, allowing them to steal data, install malware, or disrupt operations.

Affected and Fixed Versions:

Affected Versions	Fixed Versions
FortiClientLinux 7.2.0	Upgrade to 7.2.1 or above
FortiClientLinux 7.0.6 through 7.0.10	Upgrade to 7.0.11 or above
FortiClientLinux 7.0.3 through 7.0.4	Upgrade to 7.0.11 or above

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest 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://www.fortiguard.com/psirt/FG-IR-23-087