مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in FortiSwitch Devices

Tracking #:432316754

Date:16-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been discovered in multiple versions of Fortinet FortiSwitch devices.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2023-37936) has been discovered in multiple versions of Fortinet FortiSwitch devices. This vulnerability, classified as a use of hard-coded cryptographic key [CWE-321], allows a remote unauthenticated attacker in possession of the key to execute unauthorized code via crafted cryptographic request.

Vulnerability Details:

- **CVE-2023-37936**
- **CVSSv3 Score 9.6**,Severity: Critical
- The vulnerability is a use of hard-coded cryptographic key issue in Fortinet FortiSwitch devices. This type of vulnerability significantly increases the possibility that encrypted data may be recovered.
- **Affected Versions:**
  - FortiSwitch 7.4.0
  - FortiSwitch 7.2.0 through 7.2.5
  - FortiSwitch 7.0.0 through 7.0.7
  - FortiSwitch 6.4.0 through 6.4.13
  - FortiSwitch 6.2.0 through 6.2.7
  - FortiSwitch 6.0.0 through 6.0.7
- **Fixed Versions:**
  - FortiSwitch 7.4: Upgrade to 7.4.1 or above
  - FortiSwitch 7.2: Upgrade to 7.2.6 or above
  - FortiSwitch 7.0: Upgrade to 7.0.8 or above
  - FortiSwitch 6.4: Upgrade to 6.4.14 or above
  - FortiSwitch 6.2: Upgrade to 6.2.8 or above
  - FortiSwitch 6.0: Migrate to a fixed release

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update firmware versions for all affected FortiSwitch devices in the network.

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-23-260