مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Multiple Vulnerabilities in Fortinet FortiOS & FortiProxy

Tracking #:432315695

Date:13-03-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Fortinet FortiOS and FortiProxy products that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2023-42789 & CVE-2023-42790 (CVSSv3 Score: 9.3 - Critical):**
  - Description: An out-of-bounds write vulnerability and a stack-based buffer overflow vulnerability exist in the FortiOS & FortiProxy captive portal.
  - Impact: An inside attacker with access to the captive portal can potentially execute arbitrary code or commands on the system through specially crafted HTTP requests. This could lead to complete system compromise.
- **CVE-2024-23112 (CVSSv3 Score: 7.2 - High):**
  - Description: An authorization bypass vulnerability exists in FortiOS and FortiProxy SSLVPN due to user-controlled key.
  - Impact: An authenticated attacker can potentially gain access to another user's bookmarks through URL manipulation.
- **CVE-2023-46717 (CVSSv3 Score: 6.7 - Medium):**
  - Description: An improper authentication vulnerability exists in FortiOS when configured with FortiAuthenticator in HA.
  - Impact: An authenticated attacker with at least read-only permissions can potentially gain read-write access through successive login attempts.

Affected Products:
FortiOS version 7.4.0 through 7.4.1
FortiOS version 7.2.0 through 7.2.6
FortiOS version 7.0.0 through 7.0.13
FortiOS version 6.4.0 through 6.4.14
FortiOS version 6.2.0 through 6.2.15
FortiProxy version 7.4.0 through 7.4.2
FortiProxy version 7.2.0 through 7.2.8
FortiProxy version 7.0.0 through 7.0.14
FortiProxy version 2.0.0 through 2.0.13

Fixed Versions:
FortiOS version 7.4.2 or above
FortiOS version 7.2.7 or above
FortiOS version 7.0.14 or above
FortiOS version 6.4.15 or above
FortiOS version 6.2.16 or above
FortiProxy version 7.4.3 or above
FortiProxy version 7.2.9 or above
FortiProxy version 7.0.15 or above
FortiProxy version 2.0.14 or above

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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