



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates-FortiOS

Tracking #:432315947

Date:12-06-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Fortinet released a security update to address a vulnerability in FortiOS.

TECHNICAL DETAILS:

Fortinet has released security updates to address a vulnerability in FortiOS that may allow an authenticated attacker to execute unauthorized code or commands via specially crafted command line arguments.

- **CVE-2024-23110**-CVSSv3 Score,7.4 High
- Multiple Buffer Overflows in Diag Npu Command

Version	Affected	Fixed Versions
FortiOS 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiOS 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiOS 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiOS 6.2	6.2.0 through 6.2.15	Upgrade to 6.2.16 or above
FortiOS 6.0	6.0 all versions	Migrate to a fixed release

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating FortiOS to Fixed 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-23-460>