مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-FortiMail

Tracking #:432317014

Date:26-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Fortinet released security updates to address a stack buffer overflow vulnerability in FortiMail CLI, potentially allowing a privileged attacker to execute arbitrary code or commands via specially crafted CLI commands.

TECHNICAL DETAILS:

A stack buffer overflow vulnerability [CWE-121] has been identified in FortiMail CLI, potentially allowing a privileged attacker to execute arbitrary code or commands via specially crafted CLI commands.

Vulnerability Overview

- CVE ID: CVE-2024-46663
- Severity: Medium
- CVSS v3 Score: 6.5
- Impact: Escalation of Privilege
- Component: CLI
- Type: Stack Buffer Overflow (CWE-121)

Affected Products and Solutions:

FortiMail Version	Affected Range	Remediation
7.6.x	7.6.0 – 7.6.1	Upgrade to 7.6.2 or later
7.4.x	7.4.0 – 7.4.3	Upgrade to 7.4.4 or later
7.2.x	7.2.0 – 7.2.6	Upgrade to 7.2.7 or later
7.0.x	All versions	Migrate to a fixed release
6.4.x	All versions	Migrate to a fixed release

RECOMMENDATIONS:

- Upgrade affected FortiMail versions to the fixed version.
- For end-of-life versions (7.0.x, 6.4.x), migrate to supported releases

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-24-331