مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Fortinet

Tracking #:432317827

Date:17-10-2025

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 INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Fortinet has released multiple security advisories addressing high-severity vulnerabilities across various products, including FortiClientMac, FortiDLP, and FortiIsolator.

TECHNICAL DETAILS:

Fortinet has released multiple security advisories addressing high-severity vulnerabilities across various products, including FortiClientMac, FortiDLP, and FortiIsolator. These vulnerabilities, if exploited, could allow local privilege escalation, remote XML External Entity (XXE) attacks, or improper session handling leading to privilege abuse.

Organizations using affected Fortinet products are strongly advised to upgrade to the fixed versions immediately to prevent potential compromise of system integrity and sensitive information exposure.

Vulnerability Overview

1. Local Privilege Escalation in FortiClientMac (CVE-2025-57741)

- **Description:**
  An Incorrect Permission Assignment for Critical Resource vulnerability (CWE-732) exists in FortiClientMac that may allow a local attacker to execute arbitrary code or commands with elevated privileges through LaunchDaemon hijacking.Successful exploitation requires local access but could result in complete control over the affected system.
- **Impact:** Escalation of Privilege
- **Severity:** High (CVSSv3: 7.0)
- **Affected Versions & Fixes:**

Version	Affected	Fixed Version
FortiClientMac 7.4	7.4.0 – 7.4.3	Upgrade to 7.4.4 or above
FortiClientMac 7.2	7.2.0 – 7.2.11	Upgrade to 7.2.12 or above
FortiClientMac 7.0	All versions	Migrate to a fixed release

2. Critical XXE Vulnerability in Apache Tika Component (CVE-2025-54988)

- **Description:**
  A Critical XML External Entity (XXE) vulnerability in the tika-parser-pdf-module of Apache Tika (versions 1.13 to 3.2.1) affects FortiDLP products.
  An attacker could exploit this flaw using a crafted XFA file embedded in a PDF, enabling unauthorized reading of sensitive files or triggering malicious external requests.
  This issue affects multiple Tika-dependent Fortinet components.
- **Severity:** High (CVSSv3: 8.0)
- **Impact:** Information Disclosure / Remote Code Execution
- **Remediation:** Upgrade Apache Tika dependency to version 3.2.2 or higher
- **Affected Versions & Fixes:**

Version	Affected	Fixed Version
FortiDLP 12.2	12.2.1 – 12.2.2	Upgrade to 12.2.3 or above
FortiDLP 12.1	All versions	Migrate to a fixed release
FortiDLP 12.0	All versions	Migrate to a fixed release

FortiDLP 11.5	All versions	Migrate to a fixed release
FortiDLP 11.4	All versions	Migrate to a fixed release
FortiDLP 11.3	All versions	Migrate to a fixed release
FortiDLP 11.2 and below	Not affected	Not Applicable

3. Improper Session Handling in FortiIsolator (CVE-2024-33507)

- **Description:**
  An **Insufficient Session Expiration (CWE-613)** and **Incorrect Authorization (CWE-863)** flaw in FortiIsolator authentication could allow:
  - A remote unauthenticated attacker to log out active admin sessions via a crafted cookie.
  - A remote authenticated read-only user to gain write privileges, compromising system integrity.
- **Severity:** High (CVSSv3: 7.0)
- **Impact:** Privilege Escalation / Denial of Service
- **Affected Versions & Fixes:**

Version	Affected	Fixed Version
FortiIsolator 3.0	Not affected	Not Applicable
FortiIsolator 2.4	2.4.0 – 2.4.4	Upgrade to 2.4.5 or above
FortiIsolator 2.3	All versions	Migrate to a fixed release

RECOMMENDATIONS:

- Apply Patches Immediately: Upgrade affected FortiClientMac, FortiDLP, and FortiIsolator versions to the recommended fixed releases or migrate to a secure version.

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-25-664
- https://fortiguard.fortinet.com/psirt/FG-IR-25-771
- http://fortiguard.fortinet.com/psirt/FG-IR-24-062