



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Mozilla Security Updates

Tracking #:432316855

Date:02-10-2024

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 that Mozilla has released security updates to patch multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Mozilla has released security updates to address multiple vulnerabilities in its Firefox, Firefox ESR, and Thunderbird products. These vulnerabilities could potentially allow attackers to compromise user systems.

High-Severity Vulnerabilities

- **CVE-2024-9391:** This vulnerability could prevent users from exiting full-screen mode in Firefox Focus for Android, potentially leading to unexpected behavior or security risks.
- **CVE-2024-9392:** A compromised content process could potentially bypass site isolation, allowing attackers to access sensitive user data or execute malicious code.
- **CVE-2024-9393 & CVE-2024-9394:** These vulnerabilities could allow cross-origin access to PDF and JSON contents through multipart responses, potentially exposing sensitive information or enabling cross-site scripting (XSS) attacks.
- **CVE-2024-9401, CVE-2024-9402, & CVE-2024-9403:** These vulnerabilities are memory safety bugs that could potentially lead to crashes or code execution.

Fixed Versions

- **Firefox:** 131
- **Firefox ESR:** 128.3 and 115.16
- **Thunderbird:** 128.3 and 131

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Mozilla.

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.mozilla.org/en-US/security/advisories/>