مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Zero-Day Vulnerabilities Firefox browser

Tracking #:432315723

Date:25-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Mozilla recently released security updates to patch two critical zero-day vulnerabilities in the Firefox browser.

TECHNICAL DETAILS:

On March 22, 2024 Mozilla released security updates to address two critical zero-day vulnerabilities (CVE-2024-29943, CVE-2024-29944) in Firefox browser. These vulnerabilities could be exploited by attackers to remotely execute malicious code on vulnerable systems, potentially compromising user data and systems.

Vulnerabilities Details:

- **CVE-2024-29943: Out-of-bounds access via Range Analysis bypass**
  - An out-of-bounds memory access vulnerability exists in the JavaScript engine. This vulnerability can be exploited by attackers to corrupt memory and potentially execute arbitrary code.

- **CVE-2024-29944: Privileged JavaScript Execution via Event Handlers**
  - A vulnerability exists in the handling of event handlers that allows attackers to inject malicious code into privileged objects. This vulnerability can be exploited to gain complete control over the browser process.

Fixed Versions:
Firefox ESR 115.9.1
Firefox 124.0.1

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:

1. https://www.mozilla.org/en-US/security/advisories/mfsa2024-15/
2. https://www.mozilla.org/en-US/security/advisories/mfsa2024-16/