مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Mozilla Firefox

Tracking #:432318953

Date:13-05-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Mozilla has released security updates to address multiple vulnerabilities in Firefox.

TECHNICAL DETAILS:

Mozilla has released security updates to address multiple high-severity vulnerabilities in Firefox. These flaws affect core browser components including the JavaScript Engine, WebAssembly, and Profile Backup functionality, and could potentially allow memory corruption, sandbox escape, or arbitrary code execution.

Vulnerability Details
High Severity

- **CVE-2026-8388**
  Incorrect boundary conditions in the JavaScript Engine (JIT) could lead to unintended memory access or code execution.
- **CVE-2026-8389**
  JIT miscompilation in the JavaScript Engine may allow attackers to trigger unsafe behavior through crafted web content.
- **CVE-2026-8390**
  Use-after-free vulnerability in the JavaScript WebAssembly component could result in memory corruption and potential arbitrary code execution.
- **CVE-2026-8391**
  An unspecified issue in the JavaScript Engine could be exploited to compromise browser security.
- **CVE-2026-8401**
  Sandbox escape vulnerability in the Profile Backup component may allow attackers to bypass browser sandbox protections.

Fixed Versions

- Firefox 150.0.3 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends installing the latest versions 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/mfsa2026-45/