

Overall rating: Critical



This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware Mozilla published security advisories to address vulnerabilities in the following products:

- Firefox – versions prior to 125
- Firefox ESR – versions prior to 115.10

Technical Details

In some code patterns the JIT incorrectly optimized switch statements and generated code with out-of-bounds-reads. This vulnerability affects Firefox < 125 and Firefox ESR < 115.10.

Exploitability Metrics

Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify [VRM](#) with any questions or concerns you may have.

References

- CVE-2024-3852 CVE-2024-3853 CVE-2024-3854 CVE-2024-3855 CVE-2024-3856 CVE-2024-3857 CVE-2024-3858 CVE-2024-3859 CVE-2024-3860 CVE-2024-3861 CVE-2024-3862 CVE-2024-3863 CVE-2024-3864 CVE-2024-3865
- [Mozilla Security Advisory - MFSA 2024-18](#)
- [Mozilla Security Advisory - MFSA 2024-19](#)
- [Mozilla Security Advisories](#)
-