March 22, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Mozilla Foundation Security Advisory 2024-15 and Mozilla Foundation Security Advisory 2024-16 impacting Firefox and Firefox ESR. The vulnerability affects Firefox versions prior to 124.0.1 and Firefox ESR 115.9.1.

Technical Details

An attacker may be able to perform an out-of-bounds read or write on a JavaScript object by fooling range-based bounds check elimination. Additionally an attacker may be able to inject an event handler into a privileged object that would allow arbitrary JavaScript execution in the parent process.

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 this risk.

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-2024-29943, CVE-2024-23944
- Mozilla Foundation Security Advisory 2024-15
- Mozilla Foundation Security Advisory 2024-16
- VRM Vulnerability Reports