

## Overall Rating: High



This is a technical bulletin intended for technical audiences.

### Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Mozilla published security advisories to address vulnerabilities in the following products: Firefox – versions prior to 127 and Firefox ESR – versions prior to 115.12.

### Technical Details

If a specific sequence of actions is performed when opening a new tab, the triggering principal associated with the new tab may have been incorrect. The triggering principal is used to calculate many values, including the Referer and Sec- headers, meaning there is the potential for incorrect security checks within the browser in addition to incorrect or misleading information sent to remote websites.

***This bug only affects Firefox for Android. Other versions of Firefox are unaffected.***

Additionally, memory safety vulnerabilities were identified in Firefox 126, Firefox ESR 115.11, and Thunderbird 115.11. These vulnerabilities showed evidence of memory corruption and may be exploited to run arbitrary code.

#### **Exploitability Metrics**

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

This vulnerability is rated as a **HIGH** 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](mailto:VRM) with any questions or concerns you may have at [VulnerabilityandRiskManagement@gov.bc.ca](mailto:VulnerabilityandRiskManagement@gov.bc.ca).

### References

- CVE-2024-5687, CVE-2024-5688, CVE-2024-5689, CVE-2024-5690, CVE-2024-5691, CVE-2024-5692, CVE-2024-5693, CVE-2024-5694, CVE-2024-5695, CVE-2024-5696, CVE-2024-5697, CVE-2024-5698, CVE-2024-5699, CVE-2024-5700, CVE-2024-5701, CVE-2024-5702
- [Mozilla Foundation Security Advisory 2024-25](#)
- [Mozilla Foundation Security Advisory 2024-26](#)
- [VRM Vulnerability Reports](#)