November 21, 2023

Overall rating: High

This is a technical bulletin intended for technical audiences.

Summary

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

- Firefox – versions prior to 120
- Firefox for iOS – versions prior to 120
- Firefox ESR – versions prior to 115.5
- Thunderbird – versions prior to 5.0

Technical Details

On some systems—depending on the graphics settings and drivers—it was possible to force an out-of-bounds read and leak memory data into the images created on the canvas element.

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, Juniper Secure Analytics 7.5.0 UP7 IF02 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-2023-6204, CVE-2023-6205, CVE-2023-6206, CVE-2023-6207, CVE-2023-49060,
- Mozilla Security Advisory - MFSA 2023-49
- Mozilla Security Advisory - MFSA 2023-51
- Mozilla Security Advisory - MFSA 2023-50
- Mozilla Security Advisory - MFSA 2023-52
- Mozilla Security Advisories

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts