August 31, 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 a Mozilla Thunderbird vulnerability. Mozilla Thunderbird is a standalone mail and newsgroup client. The vulnerability affects versions prior to Thunderbird 102.15 and Thunderbird 115.2.

Technical Details

In general, these flaws cannot be exploited through email in the Thunderbird product because scripting is disabled when reading mail but are potentially risks in browser or browser-like contexts. The HIGH vulnerability issues are:

- When receiving rendering data over IPC mStream could have been destroyed when initialized, which could have led to a use-after-free causing a potentially exploitable crash.
- When creating a callback over IPC for showing the Color Picker window, multiple of the same callbacks could have been created at a time and eventually all simultaneously destroyed as soon as one of the callbacks finished. This could have led to a use-after-free causing a potentially exploitable crash.
- On Windows, an integer overflow could occur in RecordedSourceSurfaceCreation which resulted in a heap buffer overflow potentially leaking sensitive data that could have led to a sandbox escape. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*
- When UpdateRegExpStatics attempted to access initialStringHeap it could already have been garbage collected prior to entering the function, which could potentially have led to an exploitable crash.
- Memory safety bugs present in Firefox 116, Firefox ESR 102.14, Firefox ESR 115.1, Thunderbird 102.14, and Thunderbird 115.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.

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 with any questions or concerns you may have.

References

- CVE-2023-4573, CVE-2023-4574, CVE-2023-4575, CVE-2023-4576, CVE-2023-4577, CVE-2023-4578, CVE-2023-4580, CVE-2023-4581, CVE-2023-4582, CVE-2023-4583, CVE-2023-4584, CVE-2023-4585, CVE-2023-4051, CVE-2023-4053,
- Mozilla Foundation Security Advisory 2023-37
- Mozilla Foundation Security Advisory 2023-38
- Mozilla Foundation 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: https://bcgov.sharepoint.com/sites/CITZ-ISB/SitePages/vulnerability-reports.aspx

If you have any questions, please reach out to OCIOSecurity@gov.bc.ca