March 8, 2024

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 vulnerability. The vulnerability affects Mozilla Thunderbird versions prior to 115.8.1.

Technical Details

The encrypted subject of an email message could be incorrectly and permanently assigned to an arbitrary other email message in Thunderbird's local cache. Consequently, when replying to the contaminated email message, the user might accidentally leak the confidential subject to a third party. While this update fixes the bug and avoids future message contamination, it does not automatically repair existing contaminations. Users are advised to use the repair folder functionality, which is available from the context menu of email folders, which will erase incorrect subject assignments. This vulnerability affects Thunderbird prior to 115.8.1.

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

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-2024-1936
- Mozilla Foundation Security Advisory 2024-11
- VRM Vulnerability Reports