Security Advisory 2023-066

Mozilla Firefox and Thunderbird Zero-Day Vulnerability

September 14, 2023 — v1.1

TLP:CLEAR

History:

- *13/09/2023 — v1.0 – Initial publication*
- *14/09/2023 — v1.1 – Additional information related to impacted browsers*

Summary

On September 12, 2023, Mozilla released an emergency security update that addresses a zero-day vulnerability, which has been exploited in the wild. The vulnerability impacts its Firefox web browser and Thunderbird email client and is being tracked as CVE-2023-4863. The issue is being exploited in the wild [1].

[Update] Please note that this vulnerability also impacts other browsers and any software that uses the affected `libwebp` library. CERT-EU strongly advises users to promptly update to the fixed versions for all affected software.

Technical Details

The vulnerability is caused by a heap buffer overflow in the WebP code library (`libwebp`). This flaw allows for arbitrary code execution or can cause the browser to crash.

The CVSS score for other related vulnerabilities is between 8.8 and 9.6, indicating a critical level of severity [1].

[Update] Affected Products

- The following Mozilla products are affected from this flaw:
  - Firefox versions prior to 117.0.1
  - Firefox ESR versions prior to 115.2.1
  - Firefox ESR versions prior to 102.15.1
  - Thunderbird versions prior to 102.15.1
  - Thunderbird versions prior to 115.2.2
- Any software that uses the `libwebp` library (e.g. Signal, Telegram, 1Password for Mac, and many Android applications).

[Update] Recommendations

It is strongly advised to update to the fixed versions, if a patch is available.

- For Mozilla:
  - Firefox 117.0.1
  - Firefox ESR 115.2.1
  - Firefox ESR 102.15.1
  - Thunderbird 102.15.1
  - Thunderbird 115.2.2
- For any other software affected from this vulnerability, apply the fixes when they become available.

References

[1] https://www.mozilla.org/en-US/security/advisories/mfsa2023-40/