CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-020

Critical Vulnerabilities in Firefox

April 6, 2020 — v1.0

TLP:WHITE

History:

- *06/04/2020 — v1.0 – Initial publication*

Summary

On the 3rd of April 2020, Mozilla released an advisory concerning two critical vulnerabilities affecting Firefox browser [1]. According to Mozilla, both vulnerabilities are related to `use-after-free` bugs and have been exploited in the wild in targeted attacks. It is strongly recommended to update **Firefox** and **Firefox ESR** to the latest version available.

Technical Details

The vulnerability CVE-2020-6819 with **critical severity** is a `use-after-free` flaw, caused by a race condition while running the `nsDocShell destructor`.

The vulnerability CVE-2020-6820 with **critical severity** is a `use-after-free` flaw, caused by a race condition when handling a `ReadableStream`.

It is unclear how these vulnerabilities can be exploited, only that attacks happen right now that exploit them [2]. `ReadableStream` is used to read data streams, `nsDocShell`'s issue seems to have been caused by data not being released properly.

Products Affected

List of all affected products:

- Firefox before 74.0.1
- Firefox ESR before 68.6.1

Recommendations

Update Firefox products to the latest versions:

- Firefox 74.0.1
- Firefox ESR 68.6.1

References

[1] https://www.mozilla.org/en-US/security/advisories/mfsa2020-11/

[2] https://www.ghacks.net/2020/04/04/firefox-74-0-1-stable-out-with-important-security-fixes/