CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

**Security Advisory 2020-001**

# Critical Vulnerability in Mozilla Firefox

***January 10, 2020 — v1.0***

**TLP:WHITE**

*History:*

- *10/01/2020 — v1.0 – Initial publication*

## Summary

A critical vulnerability affecting Mozilla Firefox has been been disclosed [1]. The vulnerability identified as CVE-2019-17026 allows attackers to write to and read from memory locations that are off-limits, and could lead to information disclosures, security bypass and crashes. This vulnerability is actively being exploited in the wild.

## Technical Details

This vulnerability is a *type confusion* in the IonMonkey Just-in-Time (JIT) compiler for SpiderMonkey [2]. It could occur when a resource is accessed as a type that is different and incompatible with the original one. Depending on the type confusion, an attacker could disclose sensible information or cause crashes by accessing memory locations that are off-limits.

## Products Affected

This vulnerability actually affected the following products:

- Firefox prior 72.0.1
- Firefox ESR prior 68.4.1

## Recommendations

As this vulnerability is under active exploitation, it is highly recommended to update to the latest version of Firefox or Firefox ESR.

## References

[1] https://www.mozilla.org/en-US/security/advisories/mfsa2020-03/

[2] https://www.tenable.com/blog/cve-2019-17026-zero-day-vulnerability-in-mozilla-firefox-exploited-in-targeted-attacks