computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2016-142

Critical Firefox Vulnerability

December 1, 2016 — v1.1

History:

- *30/11/2016 — v1.0 – Initial publication*
- *01/12/2016 — v1.1 – Patches released by Mozilla and Tor Project*

Summary

On 29th of November 2016, a JavaScript code exploiting a vulnerability in Firefox has been discovered. The exploit took advantage of a bug in Firefox to allow the attacker to execute arbitrary code on the targeted system by having the victim load a web page containing malicious JavaScript and SVG code [5].

While the disclosed payload would only work on Windows, the vulnerability exists on Mac OS and Linux as well. The vulnerability also impacts Mozilla Thunderbird. Additionally, as the Tor Browser is based on Firefox engine, it is also vulnerable to the same vulnerability.

A patch from Mozilla has been issued on 30th of November 2016 [4,5]. Since the code of the exploit is public, and it is actively being used, updating Firefox and Thunderbird – as well as the Tor Browser – is highly recommended.

Technical Details

On 29th of November 2016, on Tor Project forum, users started complaining that a Javascript exploit was actively used against Tor Browser [1]. An independent researcher noticed that the exploit is almost identical to one used in 2013 to de-anonymize Tor Browser users [2]. The exploit requires JavaScript to be enabled.

The JavaScript code disclosed on the forum is exploiting a heap overflow bug, a type of buffer overflow that occurs in the heap data area. The code adjusts the memory location of the payload based on the version of Firefox being exploited and makes direct calls to `kernel32.dll`, a core part of any Windows operating system, allowing remote code execution on the target [3].

On 30th of November 2016, Mozilla provided a patch and technical details on the vulnerability [4,5]. The bug is a use-after-free vulnerability in SVG animation processing.

Vulnerable Systems

- Firefox browser from 41 and prior to 50.0.2 [4]
- Thunderbird mail clients prior to 45.5.1 [4]

- Tor Browser prior to 6.0.7 [6]

Recommendation

Update Mozilla Firefox to a version 50.0.2, Mozilla Thunderbird to version 45.5.1 and Tor-Browser to version 6.0.7. A workaround is to deactivate JavaScript on affected versions.

To deactivate JavaScript on Firefox browser:

- go to the address bar, type `about:config` and press enter;
- locate `javascript.enabled` and double-click on the `value` parameter to set it as `false`.

References

[1] Tor Project — https://lists.torproject.org/pipermail/tor-talk/2016-November/042639.html

[2] Twitter — https://twitter.com/TheWack0lian

[3] ArsTechnica — http://arstechnica.com/security/2016/11/firefox-0day-used-against-tor-users-almost-identical-to-one-fbi-used-in-2013 /

[4] Mozilla — https://www.mozilla.org/en-US/security/advisories/mfsa2016-92/

[5] Mozilla Blog — https://blog.mozilla.org/security/2016/11/30/fixing-an-svg-animation-vulnerability/

[6] Tor Project — https://blog.torproject.org/blog/tor-browser-607-released