Security Advisory Report - OBSO-1806-02

Electron Custom Protocol Handler Processing Arbitrary Command Injection (CVE-2018-1000006, CVE-2018-1000118)

Creation Date: 2018-06-07 17:20:06
Last Update: 2018-06-28 11:49:30

Summary

CVE-2018-1000006

Github Electron version Electron 1.8.2-beta.4 and earlier contains a Command Injection vulnerability in Protocol Handler that can result in command execution.
It can be summarized as the ability to use custom protocol handlers (e.g. myapp://) from a remote web page to piggyback command line arguments and insert a new switch that Electron/Chromium/Node would recognize and execute while launching the application.

This attack appears to be exploitable via the victim opening an electron protocol handler in their browser.
Electron *v1.7.12*, *v1.6.17* and *v1.8.2-beta5* were released.

It turned out that the initial patch did not take into account uppercase characters and led to a bypass in the previous patch.

CVE-2018-1000118

Follow-up was CVE-2018-1000118 which was partly fixed in 1.8.2 beta 5 (case sensitivity).

Finally https://blog.doyensec.com/2018/05/24/electron-win-protocol-handler-bug-bypass.html disclosed a fatal oversight in the blacklist introduced in beta 4, and this was fixed only with 1.8.7.

On May 16, 2018, Electron released a new update containing an improved version of the blacklist for v2.0.1, v1.8.7, and v1.7.15.

The team is actively working on a more resilient solution to prevent further bypasses.
Considering that the API change may potentially break existing apps, it makes sense to see this security improvement within a major release.

Details

Electron apps designed to run on Windows that register themselves as the default handler for a protocol, like myapp://, are vulnerable.

Such apps can be affected regardless of how the protocol is registered, e.g. using native code, the Windows registry, or Electron's app.setAsDefaultProtocolClient API.

macOS and Linux are **not vulnerable** to this issue.

Affected Products

myPortal @ Work

Partly fixed with electron 1.8.2, final fix is in work

Circuit Desktop Client for Windows and Mac

Circuit Desktop Client 1.2.3100 has the incomplete fix, and the final fix is in 1.2.3304.

Sprint 96 Emergency Patch with Desktop Application version 1.2.3304

Circuit Meeting Room client

Analysis is in work

All other Unify products do not use Electron or are not affected.

Recommended Actions

Please use the fix versions mentioned above.

References

https://electronjs.org/blog/protocol-handler-fix

https://www.zdnet.com/article/electron-critical-vulnerability-strikes-app-developers/

https://blog.doyensec.com/2018/05/24/electron-win-protocol-handler-bug-bypass.html

---

Advisory: OBSO-1806-02, status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com