Security Advisory Report - OBSO-1806-01

Electron webview Options Object Remote Node.js Integration Manipulation (CVE-2018-1000136)

Creation Date: 2018-06-01 14:45:34
Last Update: 2018-06-05 16:02:29

Summary

Electron contains a flaw that is triggered as insecure default values are set for the webview options object. This may allow a remote attacker to re-enable Node.js integration mechanisms.

Fixed in:

electron 1.7.13

electron 1.8.4

electron 2.0.0-beta.4

Priority: medium

Details

Webview Vulnerability Fix

https://www.electronjs.org/blog/webview-fix

A vulnerability has been discovered which allows Node.js integration to be re-enabled in some Electron applications that disable it. This vulnerability has been assigned the CVE identifier CVE-2018-1000136.

Affected Applications

An application is affected if ***all*** of the following are true:

1. Runs on Electron 1.7, 1.8, or a 2.0.0-beta
2. Allows execution of arbitrary remote code
3. Disables Node.js integration
4. Does not explicitly declare webviewTag: false in its webPreferences
5. Does not enable the nativeWindowOption option

6. Does not intercept new-window events and manually override event.newGuest without using the supplied options tag

Although this appears to be a minority of Electron applicatons, we encourage all applications to be upgraded as a precaution.

Mitigation

This vulnerability is fixed in today's 1.7.13, 1.8.4, and 2.0.0-beta.5 releases.

Developers who are unable to upgrade their application's Electron version can mitigate the vulnerability with the following code:

```
app.on('web-contents-created', (event, win) => {
  win.on('new-window', (event, newURL, frameName, disposition,
                        options, additionalFeatures) => {
    if (!options.webPreferences) options.webPreferences = {};
    options.webPreferences.nodeIntegration = false;
    options.webPreferences.nodeIntegrationInWorker = false;
    options.webPreferences.webviewTag = false;
    delete options.webPreferences.preload;
  })
})

// and *IF* you don't use WebViews at all,
// you might also want
app.on('web-contents-created', (event, win) => {
  win.on('will-attach-webview', (event, webPreferences, params) => {
    event.preventDefault();
  })
})Copy
```

Further Information

This vulnerability was found and reported responsibly to the Electron project by Brendan Scarvell of Trustwave SpiderLabs.

To learn more about best practices for keeping your Electron apps secure, see our security tutorial.

.....

Affected Products

Unify products are not affected.

Products using electron, but not affected

Circuit Meeting Room Client
5. Does not enable the nativeWindowOption option not true

Circuit Desktop Client for Windows and Mac
3. Disables Node.js integration not true
5. Does not enable the nativeWindowOption option not true
btw Version 1.2.3200 uses electron 1.8.4. which is the fix version

Products not affected

All other products do not use electron and are not affected.

Recommended Actions

no actions necessary

References

https://www.electronjs.org/blog/webview-fix

https://www.trustwave.com/Resources/SpiderLabs-Blog/CVE-2018-1000136---Electron-nodeIntegration-Bypass
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-1000136
https://github.com/electron/electron/commit/1a48ee28276e6588dbf4e70e58d78e7bfdc57043
https://github.com/electron/electron/commit/c2673aa970b5256eff3b61d624ad0ff225260add
https://github.com/electron/electron/pull/12271
https://github.com/electron/electron/pull/12294
https://github.com/electron/electron/releases/tag/v1.7.13
https://github.com/electron/electron/releases/tag/v1.8.4
https://github.com/electron/electron/releases/tag/v2.0.0-beta.4
https://nodesecurity.io/advisories/574
https://www.electronjs.org/blog/webview-fix

Advisory: OBSO-1806-01, 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