CERT-EU Security Advisory 2018-003

Critical Vulnerability in Electron on Windows

January 29, 2018 — v1.0

History:

- *29/01/2018 — v1.0: Initial publication*

Summary

On the 22nd of January 2018, GitHub published a fix for a remote code execution vulnerability affecting Electron applications that use custom protocol handlers [1]. An attacker could exploit the vulnerability by providing to the victim a specifically crafted link calling the custom protocol handler.

Popular applications potentially affected by the vulnerability include:

- Skype
- Atom
- Keeper
- Signal
- Twitch
- Github desktop
- Slack
- ...

A complete list of Electron applications may be found in [4]. These applications are vulnerable if they use custom protocol handlers (such as `myapp://`).

Technical Details

The vulnerability received the following CVE: CVE-2018-1000006 [2].

Electron applications designed to run on Windows that register themselves as the default handler for a protocol can be affected regardless of how the protocol is registered, e.g., using native code, the Windows registry, or Electron's `app.setAsDefaultProtocolClient` API.

The `app.setAsDefaultProtocolClient` method sets the executable as the default handler for a protocol (URI scheme such as `myapp://`). Once registered, all links with `myapp://` will be opened with the defined executable. The whole link, including protocol and parameters, will be passed to the application as a parameter.

The vulnerability is due to the way such links are handled by the library and parsed by Chromium. A proof of concept is available in public [3]:

```
myapp://?--no-sandbox --gpu-launcher=cmd.exe /c start calc
```

Products Affected

All applications using Electron libraries before versions `1.8.2-beta.4`, `1.7.11`, and `1.6.16` are affected by the vulnerability if they define custom protocol handler for their application.

MacOS and Linux applications are not affected.

Recommendations

Apply security patches for applications using Electron libraries.

References

[1] https://electronjs.org/blog/protocol-handler-fix

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000006

[3] https://twitter.com/mattaustin/status/956282917830852608

[4] https://electronjs.org/apps