CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-062

NPM Libraries Hijacked

November 5, 2021 — v1.0

TLP:WHITE

History:

- *05/11/2021 — v1.0 – Initial publication*

Summary

On November 4, malicious code was discovered in two popular NPM libraries [1] after unexpected releases have been published for the `coa` library. Hours after these new releases, the `rc` library was also found hijacked. The first library is a parser for command-line options, while the second is used as a configuration loader for applications. Malicious releases were all published on November 4, versions `2.0.3`, `2.0.4`, `2.1.1`, `2.1.3`, `3.1.3` for the `coa` library, and versions `1.2.9`, `1.3.9`, `2.3.9` for the `rc` library.

Technical Details

Both hijacked libraries target Windows Operating Systems. During the installation, a suspicious preinstall script will try to execute `compile.js` (which does not exist in the original versions of these packages). This file contains obfuscated JavaScript code attempts to launch `compile.bat`, also included in the NPM archive, which would eventually download and execute a `sdd.dll` from `pastorcryptograph[.]at` [1].

Once loaded using `regsvr32.exe -s compile.dll`, the DLL will perform various activities such as stealing passwords from various web browsers and applications (VNC clients, FTP clients, email accounts, etc.), taking screenshots, and keystroke logging.

Note: These techniques and files share similarities with the hijacked versions of the `ua-parser-js` library (see SA2021-057 [2]).

List of IOCs

- `compile.js`
- `compile.bat`
- `sdd.dll` from `coa` - SHA256: `f53ef1ed12f9ba49831ea33100083c9a92bc8adc6620f8a3b36a2d9ae2eb8591`
- `sdd.dll` from `rc` - SAH256: `26451f7f6fe297adf6738295b1dcc70f7678434ef21d8b6aad5ec00beb8a72cf`
- `pastorcryptograph[.]at`

Affected Products

- `coa` library versions `2.0.3`, `2.0.4`, `2.1.1`, `2.1.3`, `3.1.3`
- `rc` library versions `1.2.9`, `1.3.9`, `2.3.9`

Note: Not all versions contain the malicious files. Nevertheless, it is advised to consider all these versions as malicious.

Recommendations

CERT-EU recommends reverting to safe versions of the `coa` and `rc` libraries (if not automatically done):

- version `2.0.2` for `coa` library [3]
- version `1.2.8` for `rc` library [4]

CERT-EU also recommends searching for the IOCs on potentially affected devices. Any computer that has these packages installed or running should be considered compromised. All malicious files should be removed, and passwords and other secrets should be rotated as soon as possible.

References

[1] https://www.bleepingcomputer.com/news/security/popular-coa-npm-library-hijacked-to-steal-user-passwords/

[2] https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-057.pdf

[3] https://github.com/advisories/GHSA-73qr-pfmq-6rp8

[4] https://github.com/advisories/GHSA-g2q5-5433-rhrf