CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-057

NPM library UA-Parser-JS hijacked

October 26, 2021 — v1.0

TLP:WHITE

History:

- *26/10/2021 — v1.0 – Initial publication*

Summary

On October 22, CISA published an alert about malware discovered in the popular NPM library, `ua-parser-js` [1]. The hackers hijacked the library to infect Linux and Windows devices with cryptominers and password-stealing trojans in a supply-chain attack. This library is used to parse a browser's user agent to identify a visitor's browser, engine, OS, CPU, and Device type/model [2]. Moreover, it has a lot of dependent libraries [3]. The attackers hijacked the account of the developer on October 22, and published three malicious versions of the library, the `0.7.29`, `0.8.0`, and `1.0.0` [4].

Technical Details

Once the compromised library is installed on the device, a script named `preinstall.js` will identify the operating system, and will either launch a Linux shell script or a Windows batch file. For devices based on Linux operating system, the aforementioned script will check the location of the device. If the device is not located in Russia, Ukraine, Belarus, and Kazakhstan, it will download the `jsextension` [5] program from `159.148.186[.]228` and run it on the device. The `jsextension` is an XMRig Monero miner [2].

For devices based on Windows operating system, the batch file will download the same XMRig Monero cryptominer, save it as `jsextension.exe` [6], and run it. It will also download a `sdd.dll` file [7] from `citationsherbe[.]at` and save it as `create.dll`. This DLL is a password-stealing trojan that will try to steal the passwords stored on the device, targeting for example FTP clients, VNC, messaging software, email clients, and browsers. To be executed, `create.dll` should be loaded using the command line `regsvr32.exe -s create.dll`. Moreover, this DLL will run a PowerShell script to steal passwords for the Windows Credential Manager [2].

List of IOCs

- `preinstall.js`
- `jsextension` - SHA256: `ea131cc5ccf6aa6544d6cb29cdb78130feed061d2097c6903215be1499464c2e`
- `jsextension.exe` - SHA256: `7f986cd3c946f274cdec73f80b84855a77bc2a3c765d68897fbc42835629a5d5`
- `sdd.dll` - SHA256: `2a3acdcd76575762b18c18c644a745125f55ce121f742d2aad962521bc7f25fd`
- `159.148.186[.]228`
- `citationsherbe[.]at`

Affected Products

- UA-Parser-JS version 0.7.29
- UA-Parser-JS version 0.8.0
- UA-Parser-JS version 1.0.0

Recommendations

CERT-EU recommends downloading and applying the patched version of `UA-Parser-JS`, respectively `0.7.30`, `0.8.1`, `1.0.1`.

CERT-EU also recommends searching for the IOCs on potentially affected devices and firewalls. If one of the files is detected, it should be deleted immediately, the passwords/keys should be changed, and the tokens rotated.

References

[1] https://us-cert.cisa.gov/ncas/current-activity/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js

[2] https://www.bleepingcomputer.com/news/security/popular-npm-library-hijacked-to-install-password-stealers-miners/

[3] https://www.npmjs.com/package/ua-parser-js

[4] https://github.com/faisalman/ua-parser-js/issues/536#issuecomment-949742904

[5] https://www.virustotal.com/gui/file/ea131cc5ccf6aa6544d6cb29cdb78130feed061d2097c6903215be149

[6] https://www.virustotal.com/gui/file/7f986cd3c946f274cdec73f80b84855a77bc2a3c765d68897fbc428356

[7] https://www.virustotal.com/gui/file/2a3acdcd76575762b18c18c644a745125f55ce121f742d2aad962521b