



NPM UA-Parser-JS Poisoned with Trojans

CRITICALITY 

26/10/2021

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

A supply chain attack resulted in hijacking UAParser.js in the NPM library to spread malicious scripts in Linux and Windows devices.



Threat Details

On October 22nd UAParser.js in the popular NPM library was hijacked to spread a malicious script called preinstall.js to install trojans in Windows and Linux OS.

The script has two purposes based on the Operating System. For Linux OS, it will execute another script called preinstall.sh that will check the geolocation for the targeted devices to make sure that the users are not located in Russia, Ukraine, Belarus, or Kazakhstan. If the users are outside the previously specified countries, the script will download a crypto-mining program from 159[.]148[.]186.228 is called jsextension, which uses only 50% of the device CPU to avoid detection. For Windows OS, it will follow the same procedure as in Linux. Additionally, the script will download a password-stealing trojan called sdd.dll and save it as create.dll.

The trojan will steal credentials from various apps, including FTP clients, VNC, email clients, messaging software, and browsers, by loading it using regsvr32.exe -s create.dll command.



Recommendations



Prevention

- **Appendix A** contains the recommendations to prevent such attacks.



Detection

- **Appendix B** contains a sample of Indicators of compromise of this threat the full list is in the attached file.

References

Node poisoning: hijacked package delivers coin miner and credential-stealing backdoor. (2021). Retrieved from Sophos News: <https://news.sophos.com/en-us/2021/10/24/node-poisoning-hijacked-package-delivers-coin-miner-and-credential-stealing-backdoor/?cmp=30728>

Popular NPM library hijacked to install password-stealers, miners. (2021). Retrieved from BleepingComputer: <https://www.bleepingcomputer.com/news/security/popular-npm-library-hijacked-to-install-password-stealers-miners/>

Popular NPM Package Hijacked to Publish Crypto-mining Malware. (2021). Retrieved from The Hacker News: <https://thehackernews.com/2021/10/popular-npm-package-hijacked-to-publish.html>



Contact Us

Bahrain National CERT - National Cyber Security Center “NCSC”

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Centre recommends all the entities to replace the below affected versions with their patched counterparts: -

Malicious version	Fixed version
0.7.29	0.7.30
0.8.0	0.8.1
1.0.0	1.0.1



Appendix B – Indicators of Compromise

Indicators of Compromise

IP Addresses

194.76.225[.]46
185.158.250[.]216:443
45.11.180[.]153:443
194.76.225[.]61:443

URLs

[https://citationsherbe\[.\]at/sdd.dll](https://citationsherbe[.]at/sdd.dll)
[http://159\[.\]148.186\[.\]228/download/jsextension](http://159[.]148.186[.]228/download/jsextension)
[http://159\[.\]148.186\[.\]228/download/jsextension.exe](http://159[.]148.186[.]228/download/jsextension.exe)

SHA-256

30ee628504faea18dc99602971aafbc05a0b05dc964797edf49633f67cd178e2
e6cba23d350cb1f049266ddf10f872216f193c5279017408b869539df2e73c83
f4c800066e56dd32d20299c451fe6a2b60a3563f7f1915f8ca8db9916d810b5c
21e68b048024ba0cc5a2a94ecbc3a78c626ec7d5d705829a82ea4715131d0509
7f986cd3c946f274cdec73f80b84855a77bc2a3c765d68897fbc42835629a5d5
2a3acdcd76575762b18c18c644a745125f55ce121f742d2aad962521bc7f25fd
ea131cc5ccf6aa6544d6cb29cdb78130feed061d2097c6903215be1499464c2e
bb8ccdcf17761f1e86d8ebbc1a12b123929c48c5eea4739b7619bd53728d412b

File name

preinstall.js
preinstall.bat
preinstall.sh
create.dll



Appendix C – Best Practices

Bahrain National CERT team recommends organizations to implement the following security best practices.

- Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts for reading email and web browsing.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
- Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls, while prioritizing the implementation of the Top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement Strategies to mitigate cyber security incidents.
(<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)

CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.



-
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
 - Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
 - MITRE Corporation provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix D – TLP Definitions

TLP:RED = Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

TLP:GREEN = Limited disclosure, restricted to the community.

Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

TLP:WHITE = Disclosure is not limited.

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.