The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
https://www.cisa.gov/tlp
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.

DATE(S) ISSUED:
10/23/2021

SUBJECT:
A Vulnerability In an NPM Package Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in the NPM package ua-parser-js that could allow for remote code execution upon installation of the affected versions. NPM is the default package manager for the Javascript runtime environment Node.js and ua-parser-js is a popular package within NPM that is used for detecting browser, engine, OS, CPU and device type and model information from User-Agent data.

THREAT INTELLIGENCE:
There are reports of this vulnerability being actively exploited for malicious purpose.

SYSTEMS AFFECTED:
- ua-parser-js version 0.7.29, 0.8.0, and 1.0.0

RISK:
Government:
- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **Medium**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in the NPM package ua-parser-js that could allow for remote code execution upon installation of the affected versions. Malicious actors uploaded a version of ua-parser-js that contains several malicious scripts. The scripts are executed during installation and download additional malicious files that have been reported to run a cryptocurrency miner, steal saved passwords, export OS credentials, and copy the cookies database file from Chrome.

RECOMMENDATIONS:
The following actions be taken:

- Apply appropriate patches provided by NPM to vulnerable systems immediately after appropriate testing.
- All secrets and keys stored on infected machines should be rotated immediately from a different machine.
- Remind users not to download, accept or execute files from untrusted and unknown sources.
- Remind users not to visit untrusted websites or follow links provided by untrusted or unknown sources.

REFERENCES:

Github:
https://github.com/advisories/GHSA-pjwm-rvh2-c87w
https://github.com/faisalman/ua-parser-js/issues/536

NPM:
https://www.npmjs.com/package/ua-parser-js

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

TLP: WHITE

https://www.cisa.gov/tlp

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.