UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00215

NPM PACKAGE UA-PARSER-JS HIJACKED FOR RCE

DATE ISSUED: 26th October 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

NPM is the default package manager for Node.js – Javascript runtime environment and the ua-parser-js is a commonly used package attackers have hijacked to execute arbitrary code remotely when installed.

BREAKDOWN

Malicious actors have uploaded a malicious version of ua-parser-js, a commonly used package that detects browser, engine, Operating System(OS), Central Processing Unit (CPU), device type and model information from the User-Agent that will allow them to perform Remote Code Execution (RCE) attacks. During installation, scripts are executed to download additional malware which have been identified as being able to run cryptocurrency miners, steal passwords, exfiltrate OS credentials and copy Chrome's cookie database file. This vulnerability is currently known to be under exploitation in the wild and should be addressed on all affected systems immediately.

REMEDIATION STEPS

- Apply the supplied patched by NPM to the vulnerable versions on systems immediately (post testing)
- Rotate any secret keys stored on affected machined immediately from an alternative machine
- Educate users on the dangers of downloading or executing files from unknown or untrusted sources – remove the ability for users to run executable files on their machines without administrator approval.
- Educate users on the dangers of visiting untrusted websites or accessing links in email, chat or SMS messages.

REFERENCES & RESOURCES

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
CIS Advisory	