1,300 Malicious Packages Found in Popular npm JavaScript Package Manager

By Kevin Townsend on February 02, 2022

Share 发推 推荐 10

Malicious actors are using the npm registry as the start point for open source software (OSS) supply chain attacks.

Open source software offers huge potential for criminals and nation states to deliver widespread supply chain attacks. OSS registries provide a major feeding ground with easy access.

Npm, Inc., a subsidiary of Microsoft-owned GitHub, is the largest OSS registry providing JavaScript packages. It contains more than 1.8 million active packages – but has, says open-source security management firm WhiteSource, become a playground for 'malicious actors'. Over the last six months, the WhiteSource Diffend malware detection platform has reported more than 1,300 malicious packages to npm for stealing credentials, stealing crypto and running botnets.

Diffend was acquired by WhiteSource in April 2021. Its creator, Maciej Mensfeld joined WhiteSource as senior product manager.

In its NPM Threat Report (PDF), WhiteSource explains that through 2021 it tracked more than 32,000 packages uploaded to npm each month. There is even higher activity in new package versions, with an average of more than 17,000 published daily throughout 2021.

"Unfortunately," comments Rami Sass, co-founder and CEO of WhiteSource, "that popularity is being used by threat actors to spread malware and launch attacks that harm businesses and

individuals."

The size of the problem for industry and the opportunities for malicious actors are immense. It is expected that there will be more than 2 billion websites by the end of 2022, and almost 98% will be using JavaScript. Many of the developers will turn to npm to provide readymade JavaScript solutions. The problem is that downloaded npm packages don't need to be run or used – if a malicious npm is downloaded, it is automatically given permission to do whatever it wants.

These permissions apply both to packages with unintended vulnerabilities, and to packages with malicious code inserted by attackers.

WhiteSource Diffend is currently detecting around 10 malicious packages every day. Most of these are engaged in reconnaissance, actively or passively gathering information that can support future targeting. Fourteen percent, however, are designed to steal sensitive data such as credentials.

"As far as I know," Mensfeld told *SecurityWeek*, "at least until the end of 2021, there were no automatic tools on npm that would prevent anyone from uploading anything to the registry. So, if you wanted to upload a package that would remove, on download, all the data on the user's computer, you could easily do that. There are no pre-checks on the package."

WhiteSource reports its findings to npm, which removes the malicious packages from the registry. However, if a new malicious package is detected and reported on a Friday, it is not likely to be removed before the following Monday – and during this period it could potentially be downloaded thousands or even millions of times by automated registry managers. Noticeably, WhiteSource reports Friday as a popular day for new malicious packages to be uploaded to the registry.

A classic example of an OSS supply chain attack was revealed in late October 2021. Attackers inserted malicious code into three versions of ua-parser-js after seemingly taking over the developer's npm account. "Ua-parser-js is used to parse user agent strings in order to identify a user's browser, operating system (OS), device, and other attributes," explains WhiteSource. "Three new versions of this package were released in an attempt to get users to download them."

The package author responded quickly with new clean versions, but the malicious code remained within the registry for a further three hours. Ua-parser-js was being downloaded approximately 8 million times each week at the time.

"Any computer that has this package installed or running should be considered fully compromised," warned GitHub. "A computer or device with the affected software installed or running could allow a remote attacker to obtain sensitive information or take control of the system," advised CISA.

WhiteSource warns that malicious actors are actively researching the most effective ways to use npm for attacks. Since a malicious package is unlikely to remain in the registry undetected for more than a week, inactive code may be uploaded to a new or abandoned package to see whether it will be detected and how long it takes – similar in concept to malware authors testing their new malware versions on VirusTotal.

WhiteSource warns that developers who use npm (or any other OSS registry) should not blindly trust the system, should update only when confident in the content, should track changes, should run continuous integration (CI) in isolated stages, should create a security flow that matches the organization profile, and should take care of the entire SDLC.

WhiteSource, headquartered in Boston, U.S.A, was founded in 2011 by Azi Cohen (GM), Rami Sass (CEO), and Ron Rymon (executive chairman). It raised $75 million in a Series D funding round in April 2021.

Related: Cyber Insights 2022: Supply Chain

Related: 'Critical Severity' Warning: Malware Found in Widely Deployed npm Packages

Related: GitHub Confirms Another Major NPM Security Defect

Related: Vulnerability in 'netmask' npm Package Affects 280,000 Projects

Share 发推 推荐 10 RSS

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Previous Columns by Kevin Townsend:

Purple Teaming Security Management Firm PlexTrac Raises $70 Million
1,300 Malicious Packages Found in Popular npm JavaScript Package Manager
Newly Detected "StrifeWater" RAT Linked to Iranian APT
Iranian Hackers Using New PowerShell Backdoor Linked to Memento Ransomware
Cyber Insights 2022: Improving Criminal Sophistication

sponsored links

2022 ICS Cyber Security Conference | USA [Hybrid: Oct. 24-27]

2022 Singapore/APAC ICS Cyber Security Conference]

2022 CISO Forum: September 13-14 - A Virtual Event

Virtual Event Series - Security Summit Online Events by SecurityWeek

Tags:
NEWS & INDUSTRY Application Security Vulnerabilities

Search

Get the Daily Briefing

BRIEFING

Business Email Address Subscribe