Cyber Attack Cyber Security News Malware

npm Package Developer Released Sabotaged Version That Deletes Files for Users Based in Russia

By Guru - March 18, 2022 0

Several weeks ago, the developer of the "node-ipc," a popular npm package with more than a million weekly downloads has protested the Russo-Ukrainian War by releasing sabotaged versions of the library. Due to this escalating situation, the open-source and software supply chain is under security concern.

A developer's machine began to have all data and files deleted and overwritten by the 'node-ipc' package in newer versions, and not only that even also leaves new text files with peace messages.

Moreover, this npm package is used by all the primary and prominent libraries like Vue.js CLI.

Protestware

By targeting users with IP addresses located in Russia or Belarus and wiping arbitrary contents of files, the alterations introduced by RIAEvangelist affected the following versions of the library:-

- 10.1.1
- 10.1.2

These malicious versions are tracked under the:-

- **CVE-2022-23812**

Apart from this, among the most prominent node modules, node-ipc allows locally and remotely controlled inter-process communication (IPC) on all the major platforms:-

- Linux
- macOS
- Windows

A developer named Brandon Nozaki Miller (aka RIAEvangelist) released two open-source software packages on March 8th:-

- Peacenotwar
- Oneday-test

The developers likely created the packages primarily as a peaceful protest, since they add a "message of peace" to the desktop of anyone installing them.

Apart from this, in the first update (version 10.1.1), the malicious code changes were published on March 7th, and the second update (10.1.1) appeared 10 hours later (March 8th).

A major update, 11.0.0, was pushed just after less than 4 hours, removing the destructive modifications from the library but adding another dependency, "peacenotwar."

Based on its base64-encoded strings and obfuscation tactics, the code within the 'node-ipc,' specifically file "ssl-geospec.js," tries to disguise its true intention and goal.

> Using a simplified version of the code the cybersecurity researchers demonstrated how this code will overwrite all the files present on the system of the users of Russia and Belarus with a heart emoji in order to delete all data.

Here's what the Director of Developer Advocacy, Liran Tal stated:-

> "At this point, a very clear abuse and a critical supply chain security incident will occur for any system on which this npm package will be called upon if that matches a geo-location of either Russia or Belarus."

Flaw Profile

- **CVE ID:** CVE-2022-23812
- **Summary:** Embedded Malicious Code in node-ipc.
- **CWE:** CWE-506
- **GHSA ID:** GHSA-97m3-w2cp-4xx6
- **Severity:** Critical
- **CVSS Score:** 9.8

Moreover, in the latest version of node-ipc released on March 15, 2022, "peacenotwar" package is bumped from 9.1.3 to 9.1.5; the color NPM library is bundled with "colors", while STDOUT console messages are removed.

While in response, some criticized the 'node-ipc' developer for deleting and editing previous comments on the thread to attempt to 'cover up' his tracks.

However, RIAEvangelist does not guarantee that future versions of node-ipc will be safe for developers to use in their applications. In short, the developers should exercise caution before utilizing 'node-ipc' in their applications.

You can follow us on Linkedin, Twitter, Facebook for daily Cybersecurity and hacking news updates.

TAGS cyber attack cyber security news malware

Guru
https://cybersecuritynews.com
Gurubaran is a Security Consultant, Security Editor & Co-Founder of Cyber Security News & GBHackers On Security.

North Korean Hackers Exploiting a Chrome zero-day Before Patch...
Guru - March 26, 2022

Google Uncovers Initial Access Broker Behind Conti Ransomware Who Uses Phishing to Infiltrate Organization
March 22, 2022

VMware Issues Patches for Critical Flaws in OS Command Injection Vulnerability
March 25, 2022

GIMMICK Malware Attacks macOS to Attack Organizations Across Asia
March 24, 2022

Google Chrome Urgent Security Update to Patch the Actively Exploited Zero-Day Flaw
March 26, 2022