Illustria Discovers Account Takeover Vulnerability in Popular NPM Package Affecting 1000+ Organizations

TEL AVIV, ISRAEL, February 16, 2023 /EINPresswire.com/ -- Illustria, a leading software supply chain security company, announced today that its research team has discovered a popular NPM package with nearly 4 million weekly downloads vulnerable to account takeover attacks.

Illustria Discovers Account Takeover Vulnerability

“During one of our customer on-boarding processes, our system analyzed several of their manifest files and uncovered several risks, such as dependency confusion and packages that were no longer being maintained, and one finding regarding potential account takeover, which stood out and caught our customer’s attention” said Bogdan Kortnov, CTO and Co-founder at Illustria.

“Initially, we believed it to be a false positive due to our familiarity with the highly popular package, but as we validated it was confirmed that the risk was correct - a domain name associated with one of the maintainers of an NPM package with over 3.5 million weekly downloads had expired as is available for registration, which is indeed a potential account takeover for that package” he added.

Even though NPM has a mechanism that restricts user accounts to only one active email per account, the package's associated GitHub account is recoverable. And access to the GitHub account a CI/CD automation token for publishing packages automatically can be extracted from the project’s pipeline and be used to publish new packages on behalf of the NPM user account.

This disclosure aims to share the threat attacker's point of view on how easy it is to take over a popular package by acquiring an expired domain name, which in this case was extremely cheap at $8.46. It’s important to highlight the need for better security mechanisms in the open-source supply chain to protect against malicious actors and use this as a reminder to check accounts regularly and remove any unused email addresses, and restrict the scope of the permission as possible, as two-factor authentication in many instances are bypassable.

"This is a classic example of why automatic mechanisms should be in place to protect this ecosystem since we are only humans," emphasized Idan Wiener - CEO and Co-founder at Illustria.

For more information on the disclosure, please visit - https://blog.illustria.io/illustria-discovers-account-takeover-vulnerability-in-a-popular-package-affecting-1000-8aaaf61ebfc4

About Illustria
Illustria aims to promote the responsible use of open source by preventing software supply chain attacks in the development lifecycle. By bridging the gap between security teams and engineering, Illustria helps you keep your applications secure throughout their lifecycle. To experience the benefits of Illustria's solution, schedule a demo today at https://illustria.io and safeguard against supply chain attacks. For more information, please contact Sonia Awan, PR for Illustria at soniaawanpr@gmail.com

Sonia Awan
Outbloom Public Relations
+1 747-254-5705
soniaawanpr@gmail.com
Visit us on social media:
LinkedIn
