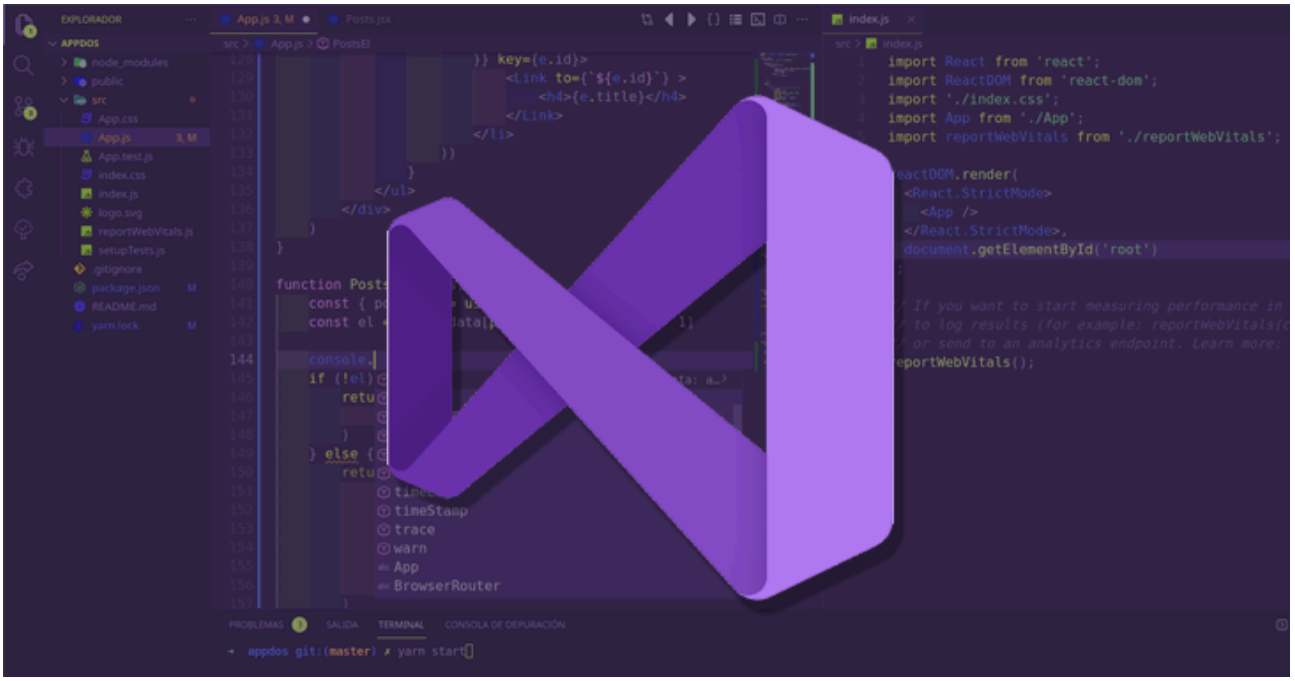
Hackers Can Abuse Visual Studio Marketplace to Target Developers with Malicious Extensions

By The Hacker News

Published: 2023-01-09 · Archived: 2026-04-05 21:38:27 UTC



A new attack vector targeting the Visual Studio Code extensions marketplace could be leveraged to upload rogue extensions masquerading as their legitimate counterparts with the goal of mounting supply chain attacks.

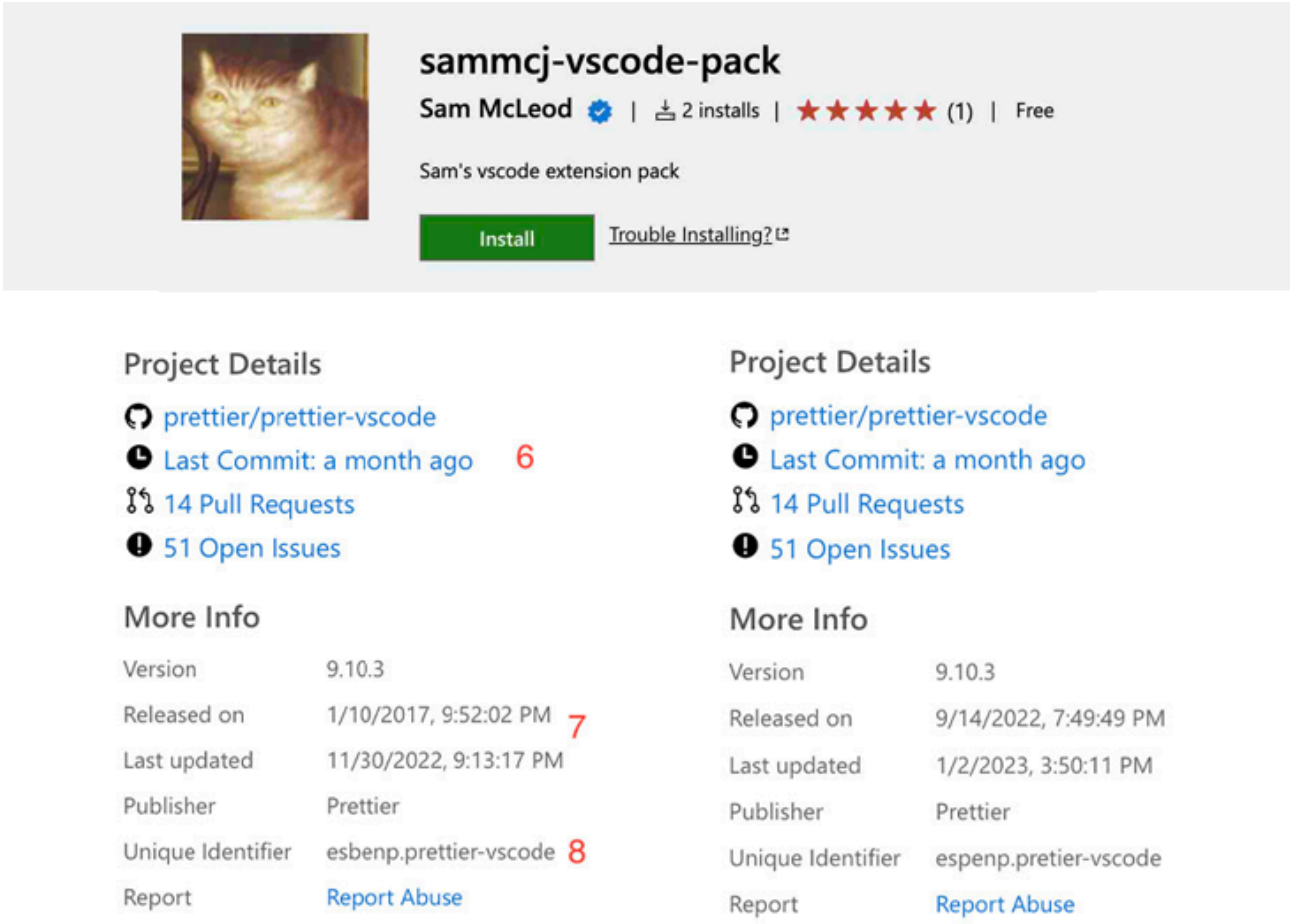
The technique "could act as an entry point for an attack on many organizations," Aqua security researcher Ilay Goldman said in a report published last week.

VS Code extensions, curated via a marketplace made available by Microsoft, allow developers to add programming languages, debuggers, and tools to the VS Code source-code editor to augment their workflows.

"All extensions run with the privileges of the user that has opened the VS Code without any sandbox," Goldman said, explaining the potential risks of using VS Code extensions. "This means that the extension can install any program on your computer including ransomwares, wipers, and more."

To that end, Aqua found that not only is it possible for a threat actor to impersonate a popular extension with small variations to the URL, the marketplace also allows the adversary to use the same name and extension publisher

details, including the project repository information.



While the method doesn't allow the number of installs and the number of stars to be replicated, the fact that there are no restrictions on the other identifying characteristics means it could be used to deceive developers.

The research also discovered that the verification badge assigned to authors could be trivially bypassed as the check mark only proves that the extension publisher is the actual owner of a domain.

In other words, a malicious actor could buy any domain, register it to get a verified check mark, and ultimately upload a trojanized extension with the same name as that of a legitimate one to the marketplace.

A proof-of-concept (PoC) extension masquerading as the Prettier code formatting utility racked up over 1,000 installations within 48 hours by developers across the world, Aqua said. It has since been taken down.

This is not the first time concerns have been raised about software supply chain threats in the VS Code extensions marketplace.

In May 2021, enterprise security firm Snyk uncovered a number of security flaws in popular VS Code extensions with millions of downloads that could have been abused by threat actors to compromise developer environments.

"Attackers are constantly working to expand their arsenal of techniques allowing them to run malicious code inside the network of organizations," Goldman said.

Update

A Microsoft spokesperson has shared the following statement with The Hacker News, noting that it provides tools for users to flag malicious extensions identified in the Marketplace. It also confirmed that the PoC add-on has been removed.

This technique involves the use of social engineering tactics to convince a victim to download a malicious extension. To help keep customers safe and protected, we scan extensions for viruses and malware before they are uploaded to the Marketplace and we check that an extension has a Marketplace certificate and verifiable

signature prior to being installed. To help make informed decisions, we recommend consumers review information, such as domain verification, ratings and feedback to prevent unwanted downloads.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
