VSCode Security: Malicious Extensions Detected- More Than 45,000 Downloads- PII Exposed, and Backdoors Enabled

By gmcdouga

Published: 2023-05-16 · Archived: 2026-04-21 02:01:32 UTC

Highlights:

1. **CloudGuard Spectral detected malicious extensions on the VSCode marketplace**
2. **Users installing these extensions were enabling attackers to steal PII records and to set remote shell to their machines**
3. **Once detected, we've alerted VSCode on these extensions. Soon after notification, they were removed by the VSCode marketplace team.**

VSCode (short for Visual Studio Code) is a popular and free source code editor developed by Microsoft. It's an efficient and customizable coding environment that can support a wide range of programming languages, frameworks, and tools. VSCode has gained much popularity in recent years and has become one of developers' most popular code editors. One of the main reasons is the VSCode Extensions Marketplace, a central hub where developers can discover and install new extensions to enhance their coding experience. The marketplace includes official Microsoft and third-party extensions developed by the community.

As for today, the marketplace includes around 50k extensions. The VSCode extensions are add-ons that can be installed to upgrade the functionality of the editor. They can be used to add new features, support new programming languages, integrate with external tools and services, and more. Malicious extensions can pose a security risk to users by installing malware, stealing user data, or performing other harmful actions.

To prevent the distribution of malicious extensions, Microsoft has implemented several security measures for the VSCode Extensions Marketplace, such as automatic extension scanning tools to detect and remove malicious extensions from the marketplace and user reviews and ratings to identify and report malicious extensions. Until this day, almost no malicious extensions were published to be detected on the VSCode marketplace.

Threat actors keep searching for new ways to infect users, and open-source code components can be a common source for infections—especially the more common ones. As such, we've decided to investigate VSCode extensions in search of malicious ones.

As part of our analysis, we found and disclosed a few malicious extensions to the VSCode team with a total count of more than 45K installs. We've also found extensions with suspicious code patterns but no clear malicious indicators. Once detected, we disclosed our findings to the VSCode team, and the extensions were removed.

These continued findings highlight the need to verify every open-source component, not just assume it will be ok. We have included details regarding our specific findings below.

The VSCode extensions marketplace

Malicious Extensions with more than 45,000 Installs

Prettiest java

The first extension to mention was named ‘prettiest java.’ Based on its short description, it was supposed to be a ‘java helper,’ probably a simple name-squatting, trying to fool users by mimicking the popular Prettier-Java code formatter project. Looking into the extension code, we could witness a classic PII stealer code, quite common on the PyPI distribution, searching for local secrets and sending them to the attacker using a Discord webhook.

The extension description from the VSCode marketplace

Theme Darcula dark

The next extension to mention was named ‘Theme Darcula dark,’ based on its description, it was supposed to be *‘an attempt to improve Dracula colors consistency on VS Code, making it more pleasant to the eyes during coding sessions.’* This extension was interesting for two reasons; first, it was quite popular, with more than 45k installs. The second is the malicious code contained within. While the extension was supposed to be a simple theme configuration (no code should be included), it had a simple PII stealer code, which is quite common among NPM malicious packages, sending much metadata regarding the installer settings to a remote machine. Code that shouldn’t exist, especially for allegedly editor theme.

Python-vscode

The last malicious extension was named ‘python-vscode.’ While the extension didn’t have a description (and therefore, most users shouldn’t even be aware of or pay attention to), witnessing its relatively high installs count indicates it managed to attract VSCode users to download and install it–effectively infecting those installers. An explanation for that is the extension naming, which can fool users into assuming it is a Python development VSCode enabler. Looking into the extension code, we faced an obfuscated statement being injected into the installer machine. Interestingly, this code was a common C# shell injector code pattern.

The extension description from the VSCode marketplace

Snippet from the extension main .js code, injecting obfuscated C# code

Probably the reference malicious code, found on Github

Suspicious but not clearly malicious

As part of our analysis, we came across multiple cases where extensions were using suspicious code patterns but, at the same time, weren't clearly malicious. The more notable cases were those using private registries to install from the required packages (instead of NPM, which can be a way to sneak in malicious packages silently) and those downloading resources from general IP addresses. Both can be theoretically abused to infect installers but currently don't seem to include clear evidence that this is the case.

Disclosure

We disclosed the malicious extensions to VSCode, and soon after, the VSCode marketplace team removed them.

Disclosure – timeline

May 4th, 2023 – disclosure submitted to VSCode

May 8th, 2023 – VSCode team acknowledged the submission

May 14th, 2023 – malicious extensions were removed from the VSCode marketplace

An increasing risk

It's important to emphasize that the malicious extensions we've found are not new; most of them are even more than a year old. This fact highlights again the open-source components risk; no one guarantees that the open sources we use are benign, and it's our responsibility to verify them.

Supply chain attacks are becoming more frequent. Therefore, it's essential to ensure we're kept safe, and to double-check every software ingredient we use, especially those we didn't create. At Check Point, we aim to generate a secure development process to ensure developers do the right things (security-wise). As part of this effort, CloudGuard Spectral constantly scans PyPI and NPM for malicious packages to prevent supply chain attack risks—keeping your code clean, applications safe, and malicious actors out.

Source: https://blog.checkpoint.com/securing-the-cloud/malicious-vscode-extensions-with-more-than-45k-downloads-steal-pii-and-enable-backdoors/