مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Malicious Code Found in VSCode Extensions

Tracking #:432316913

Date: 27-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft removed two highly popular Visual Studio Code (VSCode) extensions, 'Material Theme – Free' and 'Material Theme Icons – Free,' from the Visual Studio Marketplace after cybersecurity researchers identified malicious code within the extensions

TECHNICAL DETAILS:

On February 26, 2025, Microsoft removed two highly popular Visual Studio Code (VSCode) extensions, **'Material Theme – Free'** and **'Material Theme Icons – Free,'** from the Visual Studio Marketplace after cybersecurity researchers identified malicious code within the extensions. These extensions, developed by Mattia Astorino (aka equinusocio), had been installed nearly 9 million times collectively. Microsoft has since disabled the extensions across all VSCode instances and banned the developer from the marketplace.

The malicious code was discovered in an obfuscated JavaScript file (release-notes.js) within the extensions. Researchers suspect the code was introduced via a compromised dependency or a supply chain attack. The obfuscated code contained references to usernames and passwords, though its exact functionality remains unclear.

This incident highlights the risks associated with third-party extensions in developer tools and underscores the importance of rigorous security practices when using open-source or closed-source software.

Indicators of Compromise (IoCs)
equinusocio.moxer-theme
equinusocio.vsc-material-theme
equinusocio.vsc-material-theme-icons
equinusocio.vsc-community-material-theme
equinusocio.moxer-icons

RECOMMENDATIONS:

- Immediate Removal of Affected Extensions-Uninstall the mentioned extensions from all VSCode instances.
- Review all installed VSCode extensions for suspicious behavior or outdated dependencies.
- Stay informed about updates from Microsoft regarding this incident. Monitor the VSMarketplace GitHub repository for additional details.
- Enhance Supply Chain Security-Ensure all dependencies used in development projects are up-to-date and sourced from trusted providers.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://medium.com/extensiontotal/a-wolf-in-dark-mode-the-malicious-vs-code-theme-that-fooled-millions-85ed92b4bd26