Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

GitHub Copilot Flaw Allows Attackers to Steal Source Code from Private Repositories

Vulnerability Note: VN-2025-30

Date of Issue: 13 October 2025

Severity Rating: High

Systems Affected:

- GitHub Copilot Chat

Description

GitHub Copilot Chat is an AI assistant integrated directly into GitHub's interface. It helps developers by answering questions, explaining code, and suggesting implementations based on the project context. A critical weakness was identified in GitHub Copilot Chat, discovered in June 2025, which exposed private source code and secrets to attackers. This vulnerability could allow embedding hidden prompts in pull requests, therefore allowing attackers to exfiltrate private repository data and control Copilot's responses, including injecting malicious code suggestions or links.

Workaround
A patch rolled out by August 14, 2025, removed the ability to process Markdown image tags in chat responses. This fix closed the CSP bypass and remote prompt injection vector, restoring the confidentiality of private repository contents.

Developers are encouraged to update their Copilot Chat integrations and review pull requests for any unusual or hidden content. Continuous vigilance is necessary to safeguard AI-assisted workflows against emerging attack techniques.

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene