CERT-EU

Security Advisory 2022-084

Critical Vulnerability in Visual Studio Code

December 2, 2022 — v1.0

TLP:CLEAR

History:

- *02/12/2022 — v1.0 – Initial publication*

Summary

On November 22, Microsoft published a security advisory about a Remote Code Execution vulnerability in Visual Studio Code [1]. The severity is rated critical as a remote code execution vulnerability exists in VS Code 1.71 and earlier versions for malicious notebooks. These notebooks could use command URIs to execute arbitrary commands, including potentially dangerous commands.

Technical Details

The vulnerability was reported by Google [2] and is tracked as **CVE-2022-41034**. An attacker could, through a link or website, take over the computer of a Visual Studio Code user and any computers they were connected to via the Visual Studio Code Remote Development feature. This issue affected at least GitHub Codespaces, github.dev, the web-based Visual Studio Code for Web and to a lesser extent Visual Studio Code desktop.

Microsoft released the patch 1.72 on October 11 [3], fixing this vulnerability.

Affected Products

- Visual Studio Code 1.71 and earlier versions.

Recommendations

CERT-EU recommends to apply the patches for Visual Studio Code.

References

[1] https://github.com/microsoft/vscode/security/advisories/GHSA-q6rv-h25q-6pj6

[2] https://github.com/google/security-research/security/advisories/GHSA-pw56-c55x-cm9m

[3] https://code.visualstudio.com/updates/v1_72