



CVE-2019-16765

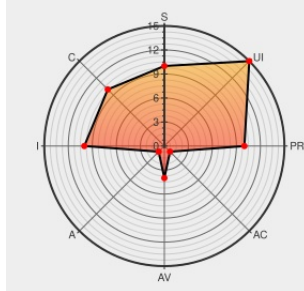
Published on: 11/25/2019 12:00:00 AM UTC

Last Modified on: 10/28/2021 01:02:00 PM UTC

CVE-2019-16765 - advisory for GHSA-wf4x-8mpj-r42q

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N



Certain versions of [Codeql](#) from [Microsoft](#) contain the following vulnerability:

If an attacker can get a user to open a specially prepared directory tree as a workspace in Visual Studio Code with the CodeQL extension active, arbitrary code of the attacker's choosing may be executed on the user's behalf. This is fixed in version 1.0.1 of the extension. Users should upgrade to this version using Visual Studio Code Marketplace's

upgrade mechanism. After upgrading, the codeQL.cli.executablePath setting can only be set in the per-user settings, and not in the per-workspace settings. More information about VS Code settings can be found [here](#).

CVE-2019-16765 has been assigned by [github](#) security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [github](#) - **vscode-codeql** version < 1.0.1

Vulnerability Patch/Work Around

Manually review the workspace settings for any workspace obtained from an external source. These settings can be found in the .vscode/settings.json file within the workspace directory. Remove the configuration values for the codeQL.cli.executablePath, codeQL.cli.owner, and codeQL.cli.repository settings for the workspace. If you wish to use the codeQL.cli.executablePath setting to indicate the location of a CodeQL CLI executable, then move this to your user settings, and check that you trust the configured path. You can access the user settings by choosing Preferences: Open User Settings from the Command Palette.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

vector	Complexity	
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Change distribution settings to machine scope by henrymercer · Pull Request #174 · github/vscode-codeql · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/github/vscode-codeql/pull/174
Arbitrary code execution when opening a malicious workspace · Advisory · github/vscode-codeql · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/github/vscode-codeql/security/advisories/GHSA-wf4x-8mpj-r42q
vscode-codeql/CHANGELOG.md at v1.0.1 · github/vscode-codeql · GitHub	Release Notes github.com text/html	MISC github.com/github/vscode-codeql/blob/v1.0.1/CHANGELOG.md

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Codeql	All	All	All	All
Application	Microsoft	Codeql	All	All	All	All
cpe:2.3:a:microsoft:codeql:*:*:*:*:visual_studio_code:*:*						
cpe:2.3:a:microsoft:codeql:*:*:*:*:visual_studio_code:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @LinInfoSec	Vscode - CVE-2019-16765: github.com/github/vscode-...	2021-10-28 14:35:19

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)