



CVE-2022-30129

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-30129
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-10 21:15:00 UTC
Updated	2023-12-20 22:15:00 UTC
Description	Visual Studio Code Remote Code Execution Vulnerability.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Visual Studio Code	All	All	All	All

References

Reference	Source	Link	Tags
Windows11Exploits/CVE-2022-30129 at main · nu11secu1ty/Windows11Exploits · GitHub	MISC	github.com	
Securing Developer Tools: Argument Injection in Visual Studio Code	MISC	blog.sonarsource.com	
CVE-2022-30129	MISC	www.nu11secu1ty.com	
Security Update Guide - Microsoft Security Response Center	MISC	portal.msrc.microsoft.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[376584](#) Microsoft Visual Studio Code Remote Code Execution (RCE) Vulnerability for May 2022

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report