



CVE-2021-22539

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

Summary

CVE	CVE-2021-22539
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-16 11:15:00 UTC
Updated	2022-10-25 16:36:00 UTC
Description	An attacker can place a crafted JSON config file into the project folder pointing to a custom executable. VScode-bazel allow

Risk And Classification

Problem Types: CWE-668

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Bazel	All	All	All	All

References

Reference	S
Malicious project can cause vscode-bazel to run arbitrary executable when linting a *.bzl file · Advisory · bazelbuild/vscode-bazel · GitHub	M
github.com/bazelbuild/vscode-bazel-ghsa-2rcw-j8x4-hgcv/pull/1	M
CVE Program record	C
NVD vulnerability detail	N

Vendor Comments And Credit

Discovery Credit
LEGACY: RyotaK

There are currently no legacy QID mappings associated with this CVE.

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