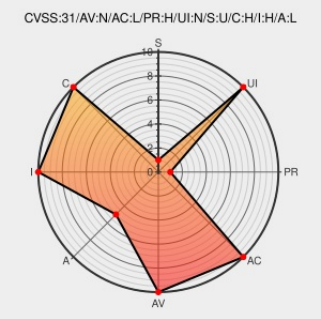
CVE-2021-3035

Published on: 04/19/2021 12:00:00 AM UTC

Last Modified on: 10/18/2021 12:14:00 PM UTC

CVE-2021-3035

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Bridgecrew Checkov from Paloaltonetworks contain the following vulnerability:

An unsafe deserialization vulnerability in Bridgecrew Checkov by Prisma Cloud allows arbitrary code execution when processing a malicious terraform file. This issue impacts Checkov 2.0 versions earlier than Checkov 2.0.26. Checkov 1.0 versions are not impacted.

CVE-2021-3035 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

Palo Alto Networks is not aware of any malicious exploitation of this issue.

Affected Vendor/Software: **Palo Alto Networks** - **Bridgecrew Checkov** version **< 2.0.26**

Affected Vendor/Software: **Palo Alto Networks** - **Bridgecrew Checkov** version **!>= 2.0.26**

Affected Vendor/Software: **Palo Alto Networks** - **Bridgecrew Checkov** version **! all**

Vulnerability Patch/Work Around

Do not run Checkov on terraform files from untrusted sources or pull requests.

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2021-3035 Bridgecrew Checkov: Unsafe deserialization of Terraform files allows code execution	security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2021-3035

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Paloaltonetworks	Bridgecrew Checkov	All	All	All	All

cpe:2.3:a:paloaltonetworks:bridgecrew_checkov:*:*:*:*:*:*:*:*:

Discovery Credit

Palo Alto Networks thanks Kevin Higgs of Trail of Bits for discovering and reporting this issue.

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→