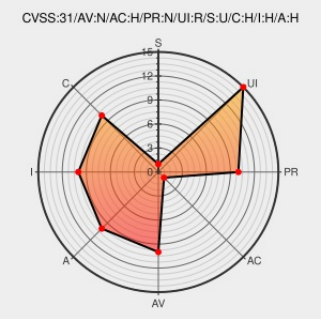
CVE-2021-3043

Published on: 07/15/2021 12:00:00 AM UTC

Last Modified on: 07/27/2021 03:12:00 PM UTC

CVE-2021-3043

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



Certain versions of Prisma Cloud from Paloaltonetworks contain the following vulnerability:

A reflected cross-site scripting (XSS) vulnerability exists in the Prisma Cloud Compute web console that enables a remote attacker to execute arbitrary JavaScript code in the browser-based web console while an authenticated administrator is using that web interface. Prisma Cloud Compute SaaS versions were automatically upgraded to the fixed release. No additional action is required for these instances. This issue impacts: Prisma Cloud Compute 20.12 versions earlier than Prisma Cloud Compute 20.12.552; Prisma Cloud Compute 21.04 versions earlier than Prisma Cloud Compute 21.04.439.

CVE-2021-3043 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as MEDIUM severity.

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

Affected Vendor/Software: **Palo Alto Networks** - **Prisma Cloud Compute** version **< 21.04.439**

Affected Vendor/Software: **Palo Alto Networks** - **Prisma Cloud Compute** version **!>= 21.04.439**

Affected Vendor/Software: **Palo Alto Networks** - **Prisma Cloud Compute** version **< 20.12.552**

Affected Vendor/Software: **Palo Alto Networks** - **Prisma Cloud Compute** version **!>= 20.12.552**

Vulnerability Patch/Work Around

There are no known workarounds for this issue.

CVSS3 Score: 4.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**

CHANGED	LOW	LOW	NONE

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
CVE-2021-3043 Prisma Cloud: Cross-Site Scripting (XSS) Vulnerability in Prisma Cloud Compute Web Console	security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2021-3043

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	Paloaltonetworks	Prisma Cloud	All	All	All	All

cpe:2.3:a:paloaltonetworks:prisma_cloud:*:*:*:*:compute:*:*:*:

Discovery Credit

This issue was found during an internal security review.

Social Mentions

Source	Title	Posted (UTC)
@autumn_good_35	『Prisma Cloud Compute SaaS versions were automatically upgraded to the fixed release.』 CVE-2021-3043 Prisma Cloud:… twitter.com/i/web/status/1…	2021-07-15 13:14:51
@CVEreport	CVE-2021-3043 : A reflected cross-site scripting #XSS vulnerability exists in the Prisma Cloud Compute web consol… twitter.com/i/web/status/1…	2021-07-15 16:48:18
/r/netcve	CVE-2021-3043	2021-07-15 17:41:10

← Previous ID

Next ID→

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