

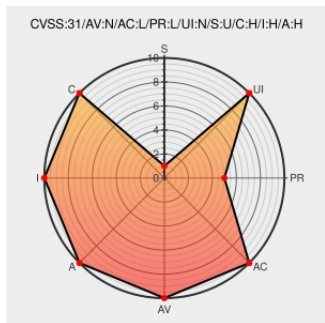


CVE-2021-44657

Published on: Not Yet Published

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-44657

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

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

In StackStorm versions prior to 3.6.0, the jinja interpreter was not run in sandbox mode and thus allows execution of unsafe system commands. Jinja does not enable sandboxed mode by default due to backwards compatibility. Stackstorm now sets sandboxed mode for jinja by default.

CVE-2021-44657 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Python vulnerabilities : Code execution in jinja templates - Podalirius	podalirius.net text/html	MISC podalirius.net/en/articles/python-vulnerabilities-code-execution-in-jinja-templates/
I use .jinja sandboxed environment by amanda11 - Pull Request	github.com	MISC github.com/StackStorm/st2/pull/5359

[Use Jinja sandboxed environment by default - Pull Request #5359 · StackStorm/st2 · GitHub](#)
[github.com](#)
[text/html](#)
[MISC github.com/StackStorm/st2/pull/5359](#)

[StackStorm v3.6.0 Released - StackStorm](#)
[stackstorm.com](#)
[text/html](#)
[MISC stackstorm.com/2021/12/16/stackstorm-v3-6-0-released/](#)

[Execute arbitrary codes in template without sandbox environment. · Issue #549 · pallets/jinja · GitHub](#)
[github.com](#)
[text/html](#)
[MISC github.com/pallets/jinja/issues/549](#)

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	Stackstorm	Stackstorm	All	All	All	All
cpe:2.3:a:stackstorm:stackstorm:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2021-44657	2021-12-15 15:38:58

[← Previous ID](#)
[Next ID →](#)