



# CVE-2020-8029

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

## Summary

<b>CVE</b>	CVE-2020-8029
<b>State</b>	PUBLIC
<b>Assigner</b>	security@suse.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-02-11 16:15:00 UTC
<b>Updated</b>	2021-02-19 16:48:00 UTC
<b>Description</b>	A Incorrect Permission Assignment for Critical Resource vulnerability in skuba of SUSE CaaS Platform 4.5 allows local att

## Risk And Classification

**Problem Types:** CWE-732

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Suse</a>	<a href="#">Caas Platform</a>	4.5	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Caas Platform</a>	4.5	All	All	All

## References

Reference	Source	Link	Tags
Bug 1177362 – VUL-0: CVE-2020-8029: skuba: Insecure handling of private key	CONFIRM	<a href="https://bugzilla.suse.com">bugzilla.suse.com</a>	Exploit, Issue Tracking, \
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Johannes Segitz of SUSE

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**