



# CVE-2019-3867

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

## Summary

<b>CVE</b>	CVE-2019-3867
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-03-18 19:15:00 UTC
<b>Updated</b>	2021-03-25 20:08:00 UTC
<b>Description</b>	A vulnerability was found in the Quay web application. Sessions in the Quay web application never expire. An attacker, able

## Risk And Classification

**Problem Types:** CWE-613

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Redhat</a>	<a href="#">Quay</a>	2.0.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Quay</a>	3.0.0	All	All	All

## References

Reference	Source	Link	Tags
1727204 – (CVE-2019-3867) CVE-2019-3867 quay: insufficient session expiration	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
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

No vendor comments have been submitted for this CVE.

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

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](#)**