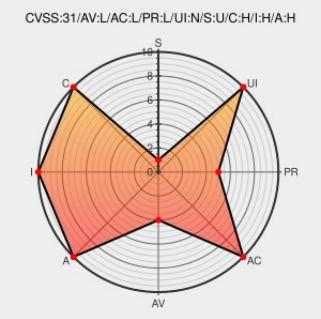
CVE-2019-3891

Published on: 04/12/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:42 PM UTC

CVE-2019-3891

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



Certain versions of Satellite from Redhat contain the following vulnerability:

It was discovered that a world-readable log file belonging to Candlepin component of Red Hat Satellite 6.4 leaked the credentials of the Candlepin database. A malicious user with local access to a Satellite host can use those credentials to modify the database and prevent Satellite from fetching package updates, thus preventing all Satellite hosts from accessing those updates.

CVE-2019-3891 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Red Hat** - **candlepin** version **affects Satellite 6.4**

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link

1693867 – (CVE-2019-3891) CVE-2019-3891 candlepin: credentials exposure through log files	Exploit Issue Tracking Mitigation Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3891
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2019:1222

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	Redhat	Satellite	6.4	All	All	All
Application	Redhat	Satellite	6.4	All	All	All

cpe:2.3:a:redhat:satellite:6.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:satellite:6.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→