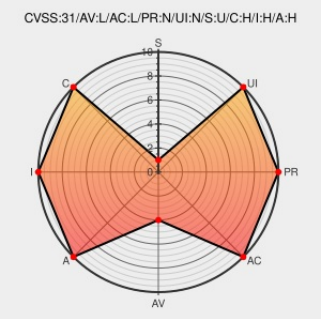
CVE-2019-18897

Published on: 03/02/2020 12:00:00 AM UTC

Last Modified on: 12/03/2022 02:20:00 AM UTC

CVE-2019-18897 - advisory for https://bugzilla.suse.com/show_bug.cgi?id=1157465

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



Certain versions of Leap from Opensuse contain the following vulnerability:

A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of salt of SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 15; openSUSE Factory allows local attackers to escalate privileges from user salt to root. This issue affects: SUSE Linux Enterprise Server 12 salt-master version 2019.2.0-46.83.1 and prior versions. SUSE Linux Enterprise Server 15 salt-master version 2019.2.0-6.21.1 and prior versions. openSUSE Factory salt-master version 2019.2.2-3.1 and prior versions.

CVE-2019-18897 has been assigned by security@suse.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **SUSE** - **SUSE Linux Enterprise Server 12** version **<= 2019.2.0-46.83.1**

Affected Vendor/Software: **SUSE** - **SUSE Linux Enterprise Server 15** version **<= 2019.2.0-6.21.1**

Affected Vendor/Software: **openSUSE** - **Factory** version **<= 2019.2.2-3.1**

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: 7.2 - HIGH

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

COMPLETE COMPLETE COMPLETE

CVE References

Description	Tags	Link
[security-announce] openSUSE-SU-2020:0357-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0357
Bug 1157465 – VUL-0: CVE-2019-18897: salt: Local privilege escalation from salt to root	Issue Tracking Vendor Advisory bugzilla.suse.com text/html	CONFIRM bugzilla.suse.com/show_bug.cgi?id=1157465

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
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Suse	Linux Enterprise Server	12	All	All	All
Operating System	Suse	Linux Enterprise Server	15	All	All	All
Operating System	Suse	Linux Enterprise Server	12	All	All	All
Operating System	Suse	Linux Enterprise Server	15	All	All	All

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:12:*:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:15:*:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:12:*:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:15:*:*:*:*:*:*:*:

Discovery Credit

Johannes Segitz

← Previous ID Next ID→

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