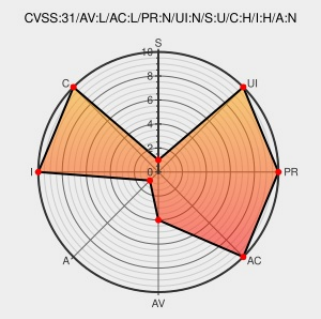
CVE-2019-3693

Published on: 01/24/2020 12:00:00 AM UTC

Last Modified on: 11/10/2022 04:42:00 AM UTC

CVE-2019-3693 - advisory for https://bugzilla.suse.com/show_bug.cgi?id=1154328

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



Certain versions of Backports Sle from Opensuse contain the following vulnerability:

A symlink following vulnerability in the packaging of mailman in SUSE Linux Enterprise Server 11, SUSE Linux Enterprise Server 12; openSUSE Leap 15.1 allowed local attackers to escalate their privileges from user wwwrun to root. Additionally arbitrary files could be changed to group mailman. This issue affects: SUSE Linux Enterprise Server 11 mailman versions prior to 2.1.15-9.6.15.1. SUSE Linux Enterprise Server 12 mailman versions prior to 2.1.17-3.11.1. openSUSE Leap 15.1 mailman version 2.1.29-lp151.2.14 and prior versions.

CVE-2019-3693 has been assigned by security@suse.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **SUSE** - **SUSE Linux Enterprise Server 11** version **< 2.1.15-9.6.15.1**

Affected Vendor/Software: **SUSE** - **SUSE Linux Enterprise Server 12** version **< 2.1.17-3.11.1**

Affected Vendor/Software: **openSUSE** - **Leap 15.1** version **<= 2.1.29-lp151.2.14**

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**

Impact	Impact	Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Bug 1154328 – VUL-0: CVE-2019-3693: mailman: LPE from wwwrun to root; ability to chgrp arbitrary files to mailman	Issue Tracking Vendor Advisory bugzilla.suse.com text/html	CONFIRM bugzilla.suse.com/show_bug.cgi?id=1154328
[security-announce] openSUSE-SU-2020:0156-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0156
[security-announce] openSUSE-SU-2020:0148-1: moderate: Security update f	Mailing List Vendor Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0148

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	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Application	Suse	Mailman	All	All	All	All
Application	Suse	Mailman	All	All	All	All
Application	Suse	Mailman	All	All	All	All

cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*:*:*:*:*:*:

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

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

cpe:2.3:o:suse:linux_enterprise_server:11:-:*:*:*:*:*:*:

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

cpe:2.3:o:suse:linux_enterprise_server:11:-:*:*:*:*:*:*:

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

cpe:2.3:a:suse:mailman:*:*:*:*:*:*:*:*:

cpe:2.3:a:suse:mailman:*:*:*:*:*:*:*:*:

cpe:2.3:a:suse:mailman:*:*:*:*:*:*:*:*:

Discovery Credit

Johannes Segitz of SUSE

← Previous ID

Next ID→

© CVE.report 2023 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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 registred 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