



CVE-2019-18903

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

Last Modified on: 03/23/2021 11:28:07 PM UTC

CVE-2019-18903 - advisory for https://bugzilla.suse.com/show_bug.cgi?id=1160904

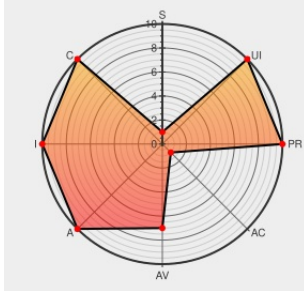
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:31/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Leap](#) from [Opensuse](#) contain the following vulnerability:

A Use After Free vulnerability in wicked of SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 15; openSUSE Leap 15.1, Factory allows remote attackers to cause DoS or potentially code execution. This issue affects: SUSE Linux Enterprise Server 12 wicked versions prior to 0.6.60-2.18.1. SUSE Linux Enterprise Server 15 wicked versions prior to 0.6.60-28.26.1. openSUSE Leap 15.1 wicked versions prior to 0.6.60-lp151.2.9.1. openSUSE Factory wicked versions prior to 0.6.62.

CVE-2019-18903 has been assigned by security@suse.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **SUSE - SUSE Linux Enterprise Server 12** version < **0.6.60-2.18.1**

Affected Vendor/Software: **SUSE - SUSE Linux Enterprise Server 15** version < **0.6.60-28.26.1**

Affected Vendor/Software: **openSUSE - Leap 15.1** version < **0.6.60-lp151.2.9.1**

Affected Vendor/Software: **openSUSE - Factory** version < **0.6.62**

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	Integrity	Availability

Impact

PARTIAL

Impact

PARTIAL

Impact

PARTIAL

CVE References

Description

Bug 1160904 – VUL-0: CVE-2019-18903: wicked: Use-after-free when receiving invalid DHCP6 IA_PD option

Tags

Issue Tracking

Vendor Advisory

bugzilla.suse.com

text/html

Link

CONFIRM

bugzilla.suse.com/show_bug.cgi?id=1160904

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	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: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

Malte Kraus

© [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 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](#)