



CVE-2018-20106

Published on: 03/15/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:35 PM UTC

CVE-2018-20106 - advisory for https://bugzilla.suse.com/show_bug.cgi?id=1114853

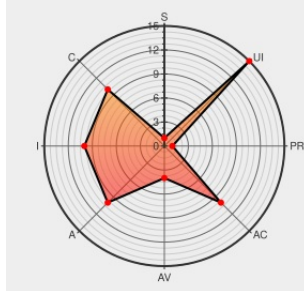
[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

CVSS:30/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H



Certain versions of **Yast2-printer** from **Opensuse** contain the following vulnerability:

In yast2-printer up to and including version 4.0.2 the SMB printer settings don't escape characters in passwords properly. If a password with backticks or simliar characters is supplied this allows for executing code as root. This requires tricking root to enter such a password in yast.

CVE-2018-20106 has been assigned by **ot** security@microfocus.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **ot SUSE** - **yast2-printer** version **4.0.2**

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Bug 1114853 – VUL-1: CVE-2018-20106: yast2-printer: SMB printer settings test	Exploit	CONFIRM

fails if the password includes a backtick

Issue Tracking

Third Party Advisory

bugzilla.suse.com

text/html

bugzilla.suse.com/show_bug.cgi?id=1114853

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	Yast2-printer	All	All	All	All
cpe:2.3:a:opensuse:yast2-printer:*:*:*:*:*:						

Discovery Credit

Dainius Masiliunas