CVE-2018-20105

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-20105
State	PUBLIC
Assigner	security@microfocus.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-27 09:15:00 UTC
Updated	2023-11-07 02:56:00 UTC
Description	A Inclusion of Sensitive Information in Log Files vulnerability in yast2-rmt of SUSE Linux Enterprise Server 15; openSUSE L

Risk And Classification

Problem Types: CWE-532

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	15	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	15	All	All	All
Application	Yast2-rmt Project	Yast2-rmt	All	All	All	All
Application	Yast2-rmt Project	Yast2-rmt	All	All	All	All

References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2020:0320-1: moderate: Security update f		lists.opensuse.org	
Bug 1119835 – VUL-0: CVE-2018-20105: yast2-rmt: CA private key passhrase exposed in log-file	CONFIRM	bugzilla.suse.com	Exploit,
[security-announce] openSUSE-SU-2020:0253-1: moderate: Security update f		lists.opensuse.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

Vendor Comments And Credit

Discovery Credit

LEGACY: Fabian Schilling of SUSE

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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