



CVE-2017-9271

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-9271
State	PUBLIC
Assigner	security@microfocus.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-01 20:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	The commandline package update tool zypper writes HTTP proxy credentials into its logfile, allowing local attackers to gain

Risk And Classification

Problem Types: CWE-532

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Opensuse	Zypper	-	All	All	All
Application	Opensuse	Zypper	-	All	All	All

References

Reference	Source	Link	Tags
Bug 1050625 – VUL-1: CVE-2017-9271: zypper: proxy credentials written to log files		bugzilla.suse.com	
[SECURITY] Fedora 33 Update: zypper-1.14.42-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
CVE-2017-9271 SUSE	CONFIRM	www.suse.com	Verified
[SECURITY] Fedora 33 Update: zypper-1.14.42-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Major
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

Vendor Comments And Credit

Discovery Credit

LEGACY: Mario Biberhofer

Legacy QID Mappings

[174846](#) SUSE Enterprise Linux Security update for libzypp, zypper (SUSE-SU-2021:0956-1)

[174865](#) SUSE Enterprise Linux Security update for libzypp, zypper (SUSE-SU-2021:0956-1)

[750435](#) OpenSUSE Security Update for libzypp, zypper (openSUSE-SU-2021:0059-1)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)