



CVE-2015-8607

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-8607
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-13 15:59:00 UTC
Updated	2020-07-15 03:15:00 UTC
Description	The canonpath function in the File::Spec module in PathTools before 3.62, as used in Perl, does not properly preserve the t

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Perl	Pathtools	All	All	All	All

References

Reference	Source
Debian -- Security Information -- DSA-3441-1 perl	DEBIAN
Perl 'File::Spec' module CVE-2015-8607 Security Bypass Vulnerability	BID
Oracle Critical Patch Update Advisory - July 2020	MISC
Document Display HPE Support Center	CONFIRM
Perl PathTools Bug in File::Spec Module Lets Remote Users Bypass Taint Restrictions on the Target System - SecurityTracker	SECTRACK
Perl: Multiple vulnerabilities (GLSA 201701-75) — Gentoo security	GENTOO
[SECURITY] Fedora 23 Update: perl-PathTools-3.60-2.fc23	FEDORA

Bug #126862 for perl5: [CVE-2015-8607] XS File::Spec::canonpath loses taint	CONFIRM
[SECURITY] Fedora 22 Update: perl-PathTools-3.47-312.fc22	FEDORA
cpansearch.perl.org/src/RJBS/PathTools-3.62/Changes	CONFIRM
openSUSE-SU-2016:0881-1: moderate: Security update for perl	SUSE
USN-2878-1: Perl vulnerability Ubuntu	UBUNTU
Oracle Critical Patch Update - July 2017	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710392](#) Gentoo Linux Perl Multiple Vulnerabilities (GLSA 201701-75)

© [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](#).

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