



CVE-2015-7236

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

Summary

CVE	CVE-2015-7236
State	PUBLIC
Assigner	security@microfocus.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-01 20:59:00 UTC
Updated	2023-11-07 02:27:00 UTC
Description	Use-after-free vulnerability in xprt_set_caller in rpcb_svc_com.c in rpcbind 0.2.1 and earlier allows remote attackers to cause

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Oracle	Solaris	10	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Application	Oracle	Solaris Operating System	10	All	All	All
Application	Oracle	Solaris Operating System	11.3	All	All	All
Application	Oracle	Solaris Operating System	10	All	All	All
Application	Oracle	Solaris Operating System	11.3	All	All	All
Application	Rpcbind Project	Rpcbind	All	All	All	All

References

Reference	Source	Link	Tag
Oracle Critical Patch Update Advisory - April 2016		www.oracle.com	
USN-2756-1: rpcbind vulnerability Ubuntu	UBUNTU	www.ubuntu.com	
Rpcbind Pointer Error Lets Remote Users Cause the Target Service to Crash - SecurityTracker		www.securitytracker.com	
oss-security - Re: CVE Request: remote triggerable use-after-free in rpcbind		www.openwall.com	
rpcbind 'rpcb_svc_com.c' Remote Memory Corruption Vulnerability	BID	www.securityfocus.com	
RPCBind: Denial of Service (GLSA 201611-17) — Gentoo security	GENTOO	security.gentoo.org	
oss-security - CVE Request: remote triggerable use-after-free in rpcbind	MLIST	www.openwall.com	
Debian -- Security Information -- DSA-3366-1 rpcbind		www.debian.org	
[SECURITY] Fedora 22 Update: rpcbind-0.2.3-0.3.fc22		lists.fedoraproject.org	
[PATCH] Fix memory corruption in PMAP_CALLIT code — Linux NFS		www.spinics.net	
FreeBSD-SA-15:24	FREEBSD	security.FreeBSD.org	
Oracle Linux Bulletin - January 2016		www.oracle.com	
[SECURITY] Fedora 23 Update: rpcbind-0.2.3-0.4.fc23	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

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

© 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