



CVE-2010-2061

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

Summary

CVE	CVE-2010-2061
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-29 22:15:00 UTC
Updated	2019-11-05 20:41:00 UTC
Description	rpcbind 0.2.0 does not properly validate (1) /tmp/portmap.xdr and (2) /tmp/rpcbind.xdr, which can be created by an attacker

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rpcbind Project	Rpcbind	0.2.0	All	All	All
Application	Rpcbind Project	Rpcbind	0.2.0	All	All	All

References

Reference	Source
#583435 - CVE-2010-2061 rpcbind: Insecure handling of state files - Debian Bug report logs	MISC
CVE-2010-2061 - Red Hat Customer Portal	MISC
CVE-2010-2061	MISC
599697 – (CVE-2010-2061, CVE-2010-2064) CVE-2010-2061 CVE-2010-2064 rpcbind: Insecure (predictable) temporary file use	MISC
oss-security - Re: CVE Request -- rpcbind -- Insecure (predictable) temporary file use	MLIST
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)