



Published on: 11/04/2002 05:00:00 AM UTC

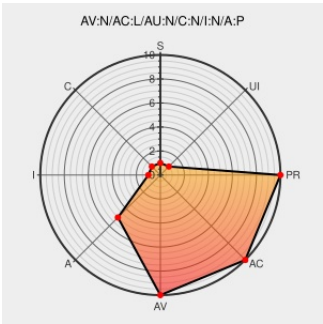
Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1232

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

Memory leak in `ypdb_open` in `yp_db.c` for `ypserv` before 2.5 in the NIS package 3.9 and earlier allows remote attackers to cause a denial of service (memory consumption) via a large number of requests for a map that does not exist.

CVE-2002-1232 has been assigned by  cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Home - Conectiva	distro.conectiva.com.br text/html	 CONECTIVA CLA-2002:539
'GLSA: ypserv' - MARC	marc.info text/html	 BUGTRAQ 20021028 GLSA: ypserv
YPServ Remote Network Information Leakage Vulnerability	Patch Vendor Advisory cve.report (archive) text/html	 BID 6016
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:229
SecurityFocus HOME Advisories: Security vulnerability in ypserv	web.archive.org text/html	 HP HPSBTL0210-074

	Inactive Link Not Archived	
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2002:224
No Description Provided	ftp.caldera.com Inactive Link Not Archived	 CALDERA CSSA-2002-054.0
ISS X-Force Database: ypserv-map-memory-leak (10423): ypserv previously existing map request memory leak	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 XF ypserv-map-memory-leak(10423)
No Description Provided	www.linux-mandrake.com Inactive Link Not Archived	 MANDRAKE MDKSA-2002:078
Debian -- Security Information -- DSA-180-1 nis	Patch Vendor Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-180
redhat.com Red Hat Support	Patch www.redhat.com text/html	 REDHAT RHSA-2002:223

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	2.2	All	All	All
Operating System	Debian	Debian Linux	2.2	All	68k	All
Operating System	Debian	Debian Linux	2.2	All	alpha	All
Operating System	Debian	Debian Linux	2.2	All	arm	All
Operating System	Debian	Debian Linux	2.2	All	ia-32	All
Operating System	Debian	Debian Linux	2.2	All	powerpc	All
Operating System	Debian	Debian Linux	2.2	All	sparc	All
Operating System	Debian	Debian Linux	3.0	All	All	All
Operating	Debian	Debian Linux	3.0	All	alpha	All

System						
Operating System	Debian	Debian Linux	3.0	All	arm	All
Operating System	Debian	Debian Linux	3.0	All	hppa	All
Operating System	Debian	Debian Linux	3.0	All	ia-64	All
Operating System	Debian	Debian Linux	3.0	All	m68k	All
Operating System	Debian	Debian Linux	3.0	All	mips	All
Operating System	Debian	Debian Linux	3.0	All	mipsel	All
Operating System	Debian	Debian Linux	3.0	All	ppc	All
Operating System	Debian	Debian Linux	3.0	All	s-390	All
Operating System	Debian	Debian Linux	3.0	All	sparc	All
Operating System	Debian	Debian Linux	2.2	All	All	All
Operating System	Debian	Debian Linux	2.2	All	68k	All
Operating System	Debian	Debian Linux	2.2	All	alpha	All
Operating System	Debian	Debian Linux	2.2	All	arm	All
Operating System	Debian	Debian Linux	2.2	All	ia-32	All
Operating System	Debian	Debian Linux	2.2	All	powerpc	All
Operating System	Debian	Debian Linux	2.2	All	sparc	All
Operating System	Debian	Debian Linux	3.0	All	All	All
Operating System	Debian	Debian Linux	3.0	All	alpha	All
Operating System	Debian	Debian Linux	3.0	All	arm	All
Operating System	Debian	Debian Linux	3.0	All	hppa	All
Operating System	Debian	Debian Linux	3.0	All	ia-64	All
Operating System	Debian	Debian Linux	3.0	All	m68k	All
Operating	Debian	Debian Linux	3.0	All	mips	All

System						
Operating System	Debian	Debian Linux	3.0	All	mipsel	All
Operating System	Debian	Debian Linux	3.0	All	ppc	All
Operating System	Debian	Debian Linux	3.0	All	s-390	All
Operating System	Debian	Debian Linux	3.0	All	sparc	All
Operating System	Hp	Secure Os	1.0	All	linux	All
Operating System	Hp	Secure Os	1.0	All	linux	All
Operating System	Redhat	Linux	6.2	All	All	All
Operating System	Redhat	Linux	6.2	All	alpha	All
Operating System	Redhat	Linux	6.2	All	i386	All
Operating System	Redhat	Linux	6.2	All	sparc	All
Operating System	Redhat	Linux	7.0	All	All	All
Operating System	Redhat	Linux	7.0	All	alpha	All
Operating System	Redhat	Linux	7.0	All	i386	All
Operating System	Redhat	Linux	7.1	All	All	All
Operating System	Redhat	Linux	7.1	All	i386	All
Operating System	Redhat	Linux	7.1	All	ia64	All
Operating System	Redhat	Linux	7.2	All	All	All
Operating System	Redhat	Linux	7.2	All	ia64	All
Operating System	Redhat	Linux	7.3	All	All	All
Operating System	Redhat	Linux	7.3	All	i386	All
Operating System	Redhat	Linux	6.2	All	All	All
Operating System	Redhat	Linux	6.2	All	alpha	All
Operating System	Redhat	Linux	6.2	All	i386	All

Operating System	Redhat	Linux	6.2	All	sparc	All
Operating System	Redhat	Linux	7.0	All	All	All
Operating System	Redhat	Linux	7.0	All	alpha	All
Operating System	Redhat	Linux	7.0	All	i386	All
Operating System	Redhat	Linux	7.1	All	All	All
Operating System	Redhat	Linux	7.1	All	i386	All
Operating System	Redhat	Linux	7.1	All	ia64	All
Operating System	Redhat	Linux	7.2	All	All	All
Operating System	Redhat	Linux	7.2	All	ia64	All
Operating System	Redhat	Linux	7.3	All	All	All
Operating System	Redhat	Linux	7.3	All	i386	All
cpe:2.3:o:debian:debian_linux:2.2:*****:						
cpe:2.3:o:debian:debian_linux:2.2:*:68k:*****:						
cpe:2.3:o:debian:debian_linux:2.2:*:alpha:*****:						
cpe:2.3:o:debian:debian_linux:2.2:*:arm:*****:						
cpe:2.3:o:debian:debian_linux:2.2:*:ia-32:*****:						
cpe:2.3:o:debian:debian_linux:2.2:*:powerpc:*****:						
cpe:2.3:o:debian:debian_linux:2.2:*:sparc:*****:						
cpe:2.3:o:debian:debian_linux:3.0:*****:						
cpe:2.3:o:debian:debian_linux:3.0:*:alpha:*****:						
cpe:2.3:o:debian:debian_linux:3.0:*:arm:*****:						
cpe:2.3:o:debian:debian_linux:3.0:*:hppa:*****:						
cpe:2.3:o:debian:debian_linux:3.0:*:ia-64:*****:						
cpe:2.3:o:debian:debian_linux:3.0:*:m68k:*****:						
cpe:2.3:o:debian:debian_linux:3.0:*:mips:*****:						

cpe:2.3:o:debian:debian_linux:3.0*:mipsel:****:
cpe:2.3:o:debian:debian_linux:3.0*:ppc:****:
cpe:2.3:o:debian:debian_linux:3.0*:s-390:****:
cpe:2.3:o:debian:debian_linux:3.0*:sparc:****:
cpe:2.3:o:debian:debian_linux:2.2*:****:
cpe:2.3:o:debian:debian_linux:2.2*:68k:****:
cpe:2.3:o:debian:debian_linux:2.2*:alpha:****:
cpe:2.3:o:debian:debian_linux:2.2*:arm:****:
cpe:2.3:o:debian:debian_linux:2.2*:ia-32:****:
cpe:2.3:o:debian:debian_linux:2.2*:powerpc:****:
cpe:2.3:o:debian:debian_linux:2.2*:sparc:****:
cpe:2.3:o:debian:debian_linux:3.0*:****:
cpe:2.3:o:debian:debian_linux:3.0*:alpha:****:
cpe:2.3:o:debian:debian_linux:3.0*:arm:****:
cpe:2.3:o:debian:debian_linux:3.0*:hppa:****:
cpe:2.3:o:debian:debian_linux:3.0*:ia-64:****:
cpe:2.3:o:debian:debian_linux:3.0*:m68k:****:
cpe:2.3:o:debian:debian_linux:3.0*:mips:****:
cpe:2.3:o:debian:debian_linux:3.0*:mipsel:****:
cpe:2.3:o:debian:debian_linux:3.0*:ppc:****:
cpe:2.3:o:debian:debian_linux:3.0*:s-390:****:
cpe:2.3:o:debian:debian_linux:3.0*:sparc:****:
cpe:2.3:o:hp:secure_os:1.0*:linux:****:
cpe:2.3:o:hp:secure_os:1.0*:linux:****:
cpe:2.3:o:redhat:linux:6.2*:****:
cpe:2.3:o:redhat:linux:6.2*:alpha:****:
cpe:2.3:o:redhat:linux:6.2*:i386:****:
cpe:2.3:o:redhat:linux:6.2*:sparc:****:
cpe:2.3:o:redhat:linux:6.2*:****:

cpe:2.3:o:redhat:linux:7.0:*:*:*:*:*:
cpe:2.3:o:redhat:linux:7.0*:alpha:*:*:*:*:
cpe:2.3:o:redhat:linux:7.0*:i386:*:*:*:*:
cpe:2.3:o:redhat:linux:7.1:*:*:*:*:*:
cpe:2.3:o:redhat:linux:7.1*:i386:*:*:*:*:
cpe:2.3:o:redhat:linux:7.1*:ia64:*:*:*:*:
cpe:2.3:o:redhat:linux:7.2:*:*:*:*:*:
cpe:2.3:o:redhat:linux:7.2*:ia64:*:*:*:*:
cpe:2.3:o:redhat:linux:7.3:*:*:*:*:*:
cpe:2.3:o:redhat:linux:7.3*:i386:*:*:*:*:
cpe:2.3:o:redhat:linux:6.2:*:*:*:*:*:
cpe:2.3:o:redhat:linux:6.2*:alpha:*:*:*:*:
cpe:2.3:o:redhat:linux:6.2*:i386:*:*:*:*:
cpe:2.3:o:redhat:linux:6.2*:sparc:*:*:*:*:
cpe:2.3:o:redhat:linux:7.0*:alpha:*:*:*:*:
cpe:2.3:o:redhat:linux:7.0*:i386:*:*:*:*:
cpe:2.3:o:redhat:linux:7.1:*:*:*:*:*:
cpe:2.3:o:redhat:linux:7.1*:i386:*:*:*:*:
cpe:2.3:o:redhat:linux:7.1*:ia64:*:*:*:*:
cpe:2.3:o:redhat:linux:7.2:*:*:*:*:*:
cpe:2.3:o:redhat:linux:7.2*:ia64:*:*:*:*:
cpe:2.3:o:redhat:linux:7.3:*:*:*:*:*:
cpe:2.3:o:redhat:linux:7.3*:i386:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)