

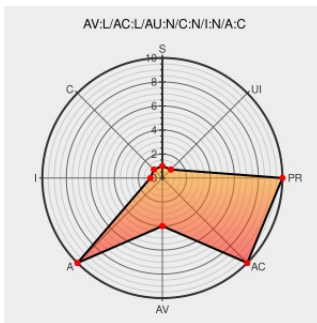


CVE-2002-2185

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:05 PM UTC

CVE-2002-2185

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The Internet Group Management Protocol (IGMP) allows local users to cause a denial of service via an IGMP membership report to a target's Ethernet address instead of the Multicast group address, which causes the target to stop sending reports to the router and effectively disconnect the group from the network.

CVE-2002-2185 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.9 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Multiple Vendor Spoofed IGMP Report Denial Of Service Vulnerability

[Exploit](#)
[Patch](#)
[cve.report \(archive\)](#)
[text/html](#)

[🌐](#) [BID 5020](#)

IGMP Denial of Service Vulnerability

[Exploit](#)
[Patch](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[UCSB](#) [MISC](#) [www.cs.ucsb.edu/~krishna/igmp_dos/](#)

Secunia - Advisories - Red Hat update for kernel

[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[X](#) [SECUNIA 18562](#)

SecurityFocus	www.securityfocus.com text/html	 FEDORA FLSA:157459-1
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF igmp-spoofed-report-dos(9436)
rhnl.redhat.com Red Hat Support	Patch www.redhat.com text/html	 REDHAT RHSA-2006:0190
SecurityFocus	www.securityfocus.com text/html	 FEDORA FLSA:157459-3
No Description Provided	patches.sgi.com Inactive Link Not Archived	 SGI 20020901-01-A
Secunia - Advisories - Red Hat update for kernel	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 18510
SecurityFocus	www.securityfocus.com text/html	 FEDORA FLSA:157459-4
SecurityFocus HOME Mailing List: BugTraq	web.archive.org text/html Inactive Link Not Archived	 BUGTRAQ 20020614 IGMP denial of service vulnerability
rhnl.redhat.com Red Hat Support	Patch www.redhat.com text/html	 REDHAT RHSA-2006:0101
Secunia - Advisories - Red Hat update for kernel	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 18684
rhnl.redhat.com Red Hat Support	Patch www.redhat.com text/html	 REDHAT RHSA-2006:0191
rhnl.redhat.com Red Hat Support	Patch www.redhat.com text/html	 REDHAT RHSA-2006:0140
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:10736
SecurityFocus	www.securityfocus.com text/html	 FEDORA FLSA:157459-2

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	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	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	Mandrakesoft	Mandrake Linux	8.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	8.0	All	ppc	All
Operating System	Mandrakesoft	Mandrake Linux	8.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	8.1	All	ia64	All
Operating System	Mandrakesoft	Mandrake Linux	8.2	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	8.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	8.0	All	ppc	All
Operating System	Mandrakesoft	Mandrake Linux	8.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	8.1	All	ia64	All
Operating System	Mandrakesoft	Mandrake Linux	8.2	All	All	All
Operating System	Microsoft	Windows 98	All	gold	All	All

Operating System	Microsoft	Windows 98	All	gold	All	All
Operating System	Microsoft	Windows 98se	All	All	All	All
Operating System	Microsoft	Windows 98se	All	All	All	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_servers	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_servers	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	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	alpha	All
Operating System	Redhat	Linux	7.0	All	i386	All
Operating System	Redhat	Linux	7.0	All	sparc	All
Operating System	Redhat	Linux	7.1	All	alpha	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	i386	All
Operating System	Redhat	Linux	7.2	All	ia64	All
Operating System	Redhat	Linux	7.3	All	i386	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	alpha	All
Operating System	Redhat	Linux	7.0	All	i386	All
Operating System	Redhat	Linux	7.0	All	sparc	All
Operating System	Redhat	Linux	7.1	All	alpha	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	i386	All
Operating System	Redhat	Linux	7.2	All	ia64	All

Operating System	Redhat	Linux	7.3	All	i386	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	ia64	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium_processor	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	ia64	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium_processor	All
Operating System	Sgi	Irix	6.5	All	All	All
Operating System	Sgi	Irix	6.5.1	All	All	All
Operating System	Sgi	Irix	6.5.10	All	All	All
Operating System	Sgi	Irix	6.5.11	All	All	All
Operating System	Sgi	Irix	6.5.12	All	All	All
Operating System	Sgi	Irix	6.5.13	All	All	All
Operating System	Sgi	Irix	6.5.14f	All	All	All
Operating System	Sgi	Irix	6.5.14m	All	All	All
Operating System	Sgi	Irix	6.5.15f	All	All	All
Operating System	Sgi	Irix	6.5.15m	All	All	All
Operating System	Sgi	Irix	6.5.16f	All	All	All
Operating System	Sgi	Irix	6.5.16m	All	All	All
Operating System	Sgi	Irix	6.5.17f	All	All	All
Operating System	Sgi	Irix	6.5.17m	All	All	All
Operating System	Sgi	Irix	6.5.18f	All	All	All
Operating System	Sgi	Irix	6.5.18m	All	All	All
Operating System	Sgi	Irix	6.5.2	All	All	All
Operating System	Sgi	Irix	6.5.3	All	All	All

Operating System	Sgi	Irix	6.5.4	All	All	All
Operating System	Sgi	Irix	6.5.5	All	All	All
Operating System	Sgi	Irix	6.5.6	All	All	All
Operating System	Sgi	Irix	6.5.7	All	All	All
Operating System	Sgi	Irix	6.5.8	All	All	All
Operating System	Sgi	Irix	6.5.9	All	All	All
Operating System	Sgi	Irix	6.5	All	All	All
Operating System	Sgi	Irix	6.5.1	All	All	All
Operating System	Sgi	Irix	6.5.10	All	All	All
Operating System	Sgi	Irix	6.5.11	All	All	All
Operating System	Sgi	Irix	6.5.12	All	All	All
Operating System	Sgi	Irix	6.5.13	All	All	All
Operating System	Sgi	Irix	6.5.14f	All	All	All
Operating System	Sgi	Irix	6.5.14m	All	All	All
Operating System	Sgi	Irix	6.5.15f	All	All	All
Operating System	Sgi	Irix	6.5.15m	All	All	All
Operating System	Sgi	Irix	6.5.16f	All	All	All
Operating System	Sgi	Irix	6.5.16m	All	All	All
Operating System	Sgi	Irix	6.5.17f	All	All	All
Operating System	Sgi	Irix	6.5.17m	All	All	All
Operating System	Sgi	Irix	6.5.18f	All	All	All
Operating System	Sgi	Irix	6.5.18m	All	All	All
Operating System	Sgi	Irix	6.5.2	All	All	All

Operating System	Sgi	Irix	6.5.3	All	All	All
Operating System	Sgi	Irix	6.5.4	All	All	All
Operating System	Sgi	Irix	6.5.5	All	All	All
Operating System	Sgi	Irix	6.5.6	All	All	All
Operating System	Sgi	Irix	6.5.7	All	All	All
Operating System	Sgi	Irix	6.5.8	All	All	All
Operating System	Sgi	Irix	6.5.9	All	All	All
Operating System	Suse	Suse Linux	6.4	All	i386	All
Operating System	Suse	Suse Linux	6.4	All	ppc	All
Operating System	Suse	Suse Linux	6.4	alpha	All	All
Operating System	Suse	Suse Linux	7.0	All	i386	All
Operating System	Suse	Suse Linux	7.0	All	ppc	All
Operating System	Suse	Suse Linux	7.0	All	sparc	All
Operating System	Suse	Suse Linux	7.0	alpha	All	All
Operating System	Suse	Suse Linux	7.1	All	spa	All
Operating System	Suse	Suse Linux	7.1	All	sparc	All
Operating System	Suse	Suse Linux	7.1	All	x86	All
Operating System	Suse	Suse Linux	7.1	alpha	All	All
Operating System	Suse	Suse Linux	7.2	All	i386	All
Operating System	Suse	Suse Linux	7.3	All	i386	All
Operating System	Suse	Suse Linux	7.3	All	ppc	All
Operating System	Suse	Suse Linux	7.3	All	sparc	All
Operating System	Suse	Suse Linux	8.0	All	i386	All

Operating System	Suse	Suse Linux	6.4	All	i386	All
Operating System	Suse	Suse Linux	6.4	All	ppc	All
Operating System	Suse	Suse Linux	6.4	alpha	All	All
Operating System	Suse	Suse Linux	7.0	All	i386	All
Operating System	Suse	Suse Linux	7.0	All	ppc	All
Operating System	Suse	Suse Linux	7.0	All	sparc	All
Operating System	Suse	Suse Linux	7.0	alpha	All	All
Operating System	Suse	Suse Linux	7.1	All	spa	All
Operating System	Suse	Suse Linux	7.1	All	sparc	All
Operating System	Suse	Suse Linux	7.1	All	x86	All
Operating System	Suse	Suse Linux	7.1	alpha	All	All
Operating System	Suse	Suse Linux	7.2	All	i386	All
Operating System	Suse	Suse Linux	7.3	All	i386	All
Operating System	Suse	Suse Linux	7.3	All	ppc	All
Operating System	Suse	Suse Linux	7.3	All	sparc	All
Operating System	Suse	Suse Linux	8.0	All	i386	All
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: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:mandrakesoft:mandrake_linux:8.0:*****:
cpe:2.3:o:mandrakesoft:mandrake_linux:8.0:*:ppc:*****:
cpe:2.3:o:mandrakesoft:mandrake_linux:8.1:*****:
cpe:2.3:o:mandrakesoft:mandrake_linux:8.1:*:ia64:*****:
cpe:2.3:o:mandrakesoft:mandrake_linux:8.2:*****:
cpe:2.3:o:mandrakesoft:mandrake_linux:8.0:*****:
cpe:2.3:o:mandrakesoft:mandrake_linux:8.0:*:ppc:*****:
cpe:2.3:o:mandrakesoft:mandrake_linux:8.1:*****:
cpe:2.3:o:mandrakesoft:mandrake_linux:8.1:*:ia64:*****:
cpe:2.3:o:mandrakesoft:mandrake_linux:8.2:*****:
cpe:2.3:o:microsoft:windows_98:*:gold:*****:
cpe:2.3:o:microsoft:windows_98:*:gold:*****:
cpe:2.3:o:microsoft:windows_98se:*****:
cpe:2.3:o:microsoft:windows_98se:*****:
cpe:2.3:o:microsoft:windows_xp:*:*:home:*****:
cpe:2.3:o:microsoft:windows_xp:*:*:gold:professional:*****:
cpe:2.3:o:microsoft:windows_xp:*:*:home:*****:
cpe:2.3:o:microsoft:windows_xp:*:*:gold:professional:*****:
cpe:2.3:o:redhat:enterprise_linux:3.0:*:advanced_servers:*****:
cpe:2.3:o:redhat:enterprise_linux:3.0:*:enterprise_server:*****:
cpe:2.3:o:redhat:enterprise_linux:3.0:*:workstation:*****:
cpe:2.3:o:redhat:enterprise_linux:4.0:*:advanced_server:*****:
cpe:2.3:o:redhat:enterprise_linux:4.0:*:enterprise_server:*****:
cpe:2.3:o:redhat:enterprise_linux:4.0:*:workstation:*****:
cpe:2.3:o:redhat:enterprise_linux:3.0:*:advanced_servers:*****:

cpe:2.3:o:redhat:enterprise_linux:3.0:*:enterprise_server:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux:3.0:*:workstation:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux:4.0:*:advanced_server:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux:4.0:*:enterprise_server:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux:4.0:*:workstation:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop:3.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop:4.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop:3.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop:4.0:*:*:*:*:*:
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:7.0:*:sparc:*:*:*:*:
cpe:2.3:o:redhat:linux:7.1:*:alpha:*:*:*:*:
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:*:i386:*:*:*:*:
cpe:2.3:o:redhat:linux:7.2:*:ia64:*:*:*:*:
cpe:2.3:o:redhat:linux:7.3:*:i386:*:*:*:*:
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:7.0:*:sparc:*:*:*:*:
cpe:2.3:o:redhat:linux:7.1:*:alpha:*:*:*:*:

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:*:i386:*****:
cpe:2.3:o:redhat:linux:7.2:*:ia64:*****:
cpe:2.3:o:redhat:linux:7.3:*:i386:*****:
cpe:2.3:o:redhat:linux_advanced_workstation:2.1:*:ia64:*****:
cpe:2.3:o:redhat:linux_advanced_workstation:2.1:*:itanium_processor:*****:
cpe:2.3:o:redhat:linux_advanced_workstation:2.1:*:ia64:*****:
cpe:2.3:o:redhat:linux_advanced_workstation:2.1:*:itanium_processor:*****:
cpe:2.3:o:sgi:irix:6.5:*****:
cpe:2.3:o:sgi:irix:6.5.1:*****:
cpe:2.3:o:sgi:irix:6.5.10:*****:
cpe:2.3:o:sgi:irix:6.5.11:*****:
cpe:2.3:o:sgi:irix:6.5.12:*****:
cpe:2.3:o:sgi:irix:6.5.13:*****:
cpe:2.3:o:sgi:irix:6.5.14f:*****:
cpe:2.3:o:sgi:irix:6.5.14m:*****:
cpe:2.3:o:sgi:irix:6.5.15f:*****:
cpe:2.3:o:sgi:irix:6.5.15m:*****:
cpe:2.3:o:sgi:irix:6.5.16f:*****:
cpe:2.3:o:sgi:irix:6.5.16m:*****:
cpe:2.3:o:sgi:irix:6.5.17f:*****:
cpe:2.3:o:sgi:irix:6.5.17m:*****:
cpe:2.3:o:sgi:irix:6.5.18f:*****:
cpe:2.3:o:sgi:irix:6.5.18m:*****:
cpe:2.3:o:sgi:irix:6.5.2:*****:
cpe:2.3:o:sgi:irix:6.5.3:*****:
cpe:2.3:o:sgi:irix:6.5.4:*****:
cpe:2.3:o:sgi:irix:6.5.5:*****:

```
cpe:2.3:o:sgi:irix:6.5.6:*.:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.7:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.8:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.9:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.1:*.:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.10:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.11:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.12:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.13:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.14f:*:*:*:*:*:
```

cpe:2.3:o:sgi:irix:6.5.14m:*:*:*:*:*:*:

```
cpe:2.3:o:sgi:irix:6.5.15f:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.15m:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.16f:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.16m:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.17f:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.17m:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.18f:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.18m:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.4:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.5:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.6:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.7:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.8:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.9:*:*:*:*:*:*:
```

cpe:2.3:o:suse:suse_linux:6.4:*:i386:*****:
cpe:2.3:o:suse:suse_linux:6.4:*:ppc:*****:
cpe:2.3:o:suse:suse_linux:6.4:alpha:*****:
cpe:2.3:o:suse:suse_linux:7.0:*:i386:*****:
cpe:2.3:o:suse:suse_linux:7.0:*:ppc:*****:
cpe:2.3:o:suse:suse_linux:7.0:*:sparc:*****:
cpe:2.3:o:suse:suse_linux:7.0:alpha:*****:
cpe:2.3:o:suse:suse_linux:7.1:*:spa:*****:
cpe:2.3:o:suse:suse_linux:7.1:*:sparc:*****:
cpe:2.3:o:suse:suse_linux:7.1:*:x86:*****:
cpe:2.3:o:suse:suse_linux:7.1:alpha:*****:
cpe:2.3:o:suse:suse_linux:7.2:*:i386:*****:
cpe:2.3:o:suse:suse_linux:7.3:*:i386:*****:
cpe:2.3:o:suse:suse_linux:7.3:*:ppc:*****:
cpe:2.3:o:suse:suse_linux:7.3:*:sparc:*****:
cpe:2.3:o:suse:suse_linux:8.0:*:i386:*****:
cpe:2.3:o:suse:suse_linux:6.4:*:i386:*****:
cpe:2.3:o:suse:suse_linux:6.4:*:ppc:*****:
cpe:2.3:o:suse:suse_linux:6.4:alpha:*****:
cpe:2.3:o:suse:suse_linux:7.0:*:i386:*****:
cpe:2.3:o:suse:suse_linux:7.0:*:ppc:*****:
cpe:2.3:o:suse:suse_linux:7.0:*:sparc:*****:
cpe:2.3:o:suse:suse_linux:7.0:alpha:*****:
cpe:2.3:o:suse:suse_linux:7.1:*:spa:*****:
cpe:2.3:o:suse:suse_linux:7.1:*:sparc:*****:
cpe:2.3:o:suse:suse_linux:7.1:*:x86:*****:
cpe:2.3:o:suse:suse_linux:7.1:alpha:*****:
cpe:2.3:o:suse:suse_linux:7.2:*:i386:*****:
cpe:2.3:o:suse:suse_linux:7.3:*:i386:*****:

cpe:2.3:o:suse:suse_linux:7.3:*:ppc:*****:	
cpe:2.3:o:suse:suse_linux:7.3:*:sparc:*****:	
cpe:2.3:o:suse:suse_linux:8.0:*:i386:*****:	
No vendor comments have been submitted for this CVE	
← Previous ID	Next ID→