



CVE-2002-1323

Published on: 12/11/2002 05:00:00 AM UTC

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

CVE-2002-1323

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

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

Safe.pm 2.0.7 and earlier, when used in Perl 5.8.0 and earlier, may allow attackers to break out of safe compartments in (1) Safe::reval or (2) Safe::rdo using a redefined @_ variable, which is not reset between successive calls.

CVE-2002-1323 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Safe.PM Unsafe Code Execution Vulnerability

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

[🌐](#) [BID 6111](#)

No Description Provided

[www.osvdb.org](#)

[🌐](#) [OSVDB 2183](#)

[Inactive Link](#) [Not Archived](#)

Debian -- Security Information -- DSA-208-1 perl

[Patch](#)
[Vendor Advisory](#)
[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[🌐](#) [DEBIAN DSA-208](#)

'GLSA: perl' - MARC

[marc.info](#)
[text/html](#)

[🌐](#) [BUGTRAQ 20021220 GLSA: perl](#)

	text/html	
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:256
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:1160
use Perl Security hole found in the Safe module	Patch web.archive.org text/html Inactive Link Not Archived	 CONFIRM use.perl.org/articles/02/10/06/1118222.shtml?tid=5
	ftp.sco.com text/plain	 SCO SCOSA-2004.1
'TSLSA-2002-0087 - perl' - MARC	marc.info text/html	 BUGTRAQ 20021219 TSLSA-2002-0087 - perl
Security-Hole in module Safe.pm · Issue #5975 · Perl/perl5 · GitHub	bugs6.perl.org text/html	 CONFIRM bugs6.perl.org/rt2/Ticket/Display.html?id=17744
Neohapsis Archives - VulnWatch - [VulnWatch] Perl Safe.pm compartment reuse vuln - From rfp_at_vulnwatch.org	web.archive.org text/html Inactive Link Not Archived	 VULNWATCH 20021105 Perl Safe.pm compartment reuse vuln
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 3814
No Description Provided	patches.sgi.com Inactive Link Not Archived	 SGI 20030606-01-A
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:257
ISS X-Force Database: safe-pm-bypass-restrictions (10574): Safe.pm could allow an attacker to bypass access restrictions	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 XF safe-pm-bypass-restrictions(10574)
No Description Provided	ftp.caldera.com Inactive Link Not Archived	 CALDERA CSSA-2004-007.0
'[OpenPKG-SA-2002.014] OpenPKG Security Advisory (perl)' - MARC	marc.info text/html	 BUGTRAQ 20021216 [OpenPKG-SA-2002.014] OpenPKG Security Advisory (perl)
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	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating	Redhat	Enterprise Linux	2.1	All	advanced_server_ia64	All

System						
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation_ia64	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	All	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	All	All
Application	Safe.pm	Safe.pm	2.0_6	All	All	All
Application	Safe.pm	Safe.pm	2.0_7	All	All	All
Application	Safe.pm	Safe.pm	2.0_6	All	All	All
Application	Safe.pm	Safe.pm	2.0_7	All	All	All
Operating System	Sco	Open Unix	8.0	All	All	All
Operating System	Sco	Open Unix	8.0	All	All	All
Operating System	Sco	Unixware	7.1.2	All	All	All
Operating System	Sco	Unixware	7.1.3	All	All	All
Operating System	Sco	Unixware	7.1.2	All	All	All
Operating System	Sco	Unixware	7.1.3	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	6.5.14	All	All	All
Operating System	Sgi	Irix	6.5.15	All	All	All
Operating System	Sgi	Irix	6.5.16	All	All	All
Operating System	Sgi	Irix	6.5.17	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	6.5.18	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	6.5.19	All	All	All
Operating System	Sgi	Irix	6.5.19f	All	All	All
Operating System	Sgi	Irix	6.5.19m	All	All	All
Operating System	Sgi	Irix	6.5.2	All	All	All
Operating System	Sgi	Irix	6.5.20f	All	All	All
Operating System	Sgi	Irix	6.5.20m	All	All	All
Operating System	Sgi	Irix	6.5.21f	All	All	All
Operating System	Sgi	Irix	6.5.21m	All	All	All
Operating System	Sgi	Irix	6.5.22	All	All	All
Operating Svstem	Sgi	Irix	6.5.3	All	All	All

System						
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	6.5.14	All	All	All
Operating System	Sgi	Irix	6.5.15	All	All	All
Operating System	Sgi	Irix	6.5.16	All	All	All
Operating System	Sgi	Irix	6.5.17	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	6.5.18	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	6.5.19	All	All	All
Operating System	Sgi	Irix	6.5.19f	All	All	All

System						
Operating System	Sgi	Irix	6.5.19m	All	All	All
Operating System	Sgi	Irix	6.5.2	All	All	All
Operating System	Sgi	Irix	6.5.20f	All	All	All
Operating System	Sgi	Irix	6.5.20m	All	All	All
Operating System	Sgi	Irix	6.5.21f	All	All	All
Operating System	Sgi	Irix	6.5.21m	All	All	All
Operating System	Sgi	Irix	6.5.22	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
Application	Sun	Linux	5.0.7	All	All	All
Application	Sun	Linux	5.0.7	All	All	All
Operating System	Sun	Solaris	8.0	All	x86	All
Operating System	Sun	Solaris	9.0	All	sparc	All
Operating System	Sun	Solaris	9.0	All	x86	All
Operating System	Sun	Solaris	8.0	All	x86	All
Operating System	Sun	Solaris	9.0	All	sparc	All
Operating System	Sun	Solaris	9.0	All	x86	All
Operating System	Sun	Sunos	5.8	All	All	All
Operating System	Sun	Sunos	5.8	All	All	All

Operating System	OS	OS	OS	OS	OS	OS
cpe:2.3:o:redhat:enterprise_linux:2.1:*:advanced_server:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1:*:advanced_server_ia64:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1:*:enterprise_server:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1:*:enterprise_server_ia64:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1:*:workstation:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1:*:workstation_ia64:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1:*:advanced_server:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1:*:advanced_server_ia64:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1:*:enterprise_server:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1:*:enterprise_server_ia64:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1:*:workstation:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1:*:workstation_ia64:*:*:*:*:						
cpe:2.3:o:redhat:linux_advanced_workstation:2.1:*:*:*:*:*:						
cpe:2.3:o:redhat:linux_advanced_workstation:2.1:*:*:*:*:*:						
cpe:2.3:a:safe.pm:safe.pm:2.0_6:*:*:*:*:*:						
cpe:2.3:a:safe.pm:safe.pm:2.0_7:*:*:*:*:*:						
cpe:2.3:a:safe.pm:safe.pm:2.0_6:*:*:*:*:*:						
cpe:2.3:a:safe.pm:safe.pm:2.0_7:*:*:*:*:*:						
cpe:2.3:o:sco:open_unix:8.0:*:*:*:*:*:						
cpe:2.3:o:sco:open_unix:8.0:*:*:*:*:*:						
cpe:2.3:o:sco:unixware:7.1.2:*:*:*:*:*:						
cpe:2.3:o:sco:unixware:7.1.3:*:*:*:*:*:						
cpe:2.3:o:sco:unixware:7.1.2:*:*:*:*:*:						
cpe:2.3:o:sco:unixware:7.1.3:*:*:*:*:*:						
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:6.5.1:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.12:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.13:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.14:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.15:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.16:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.17:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.17f:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.17m:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.18:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.18f:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.18m:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.19:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.19f:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.19m:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.2:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.20f:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.20m:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.21f:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.21m:*.***:*.***:*
cpe:2.3:o:sgi:irix:6.5.22:*.***:*.***:*
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:6.5.14:*:*:*:*:*:
```

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

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

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

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

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

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

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

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

```
cpe:2.3:o:sgi:irix:6.5.19:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.19f:*:*:*:*:*:
```

cpe:2.3:o:sgi:irix:6.5.19m:*:*:*:*:*:*

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

```
cpe:2.3:o:sgi:irix:6.5.20f:*:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.20m:*.:*:*:*:*:*:
```

```
cpe:2.3:o:sgi:irix:6.5.21f:*:*:*:*:*:
```

cpe:2.3:o:sgi:irix:6.5.21m:*:*:*:*:*:*:

```
cpe:2.3:o:sgi:irix:6.5.22:*:*:*:*:*:*:
```

```
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:*:*:*:*:*:*:
```

[illegible]

cpe:2.3:o:sgi:irix:6.5.8:*****:
cpe:2.3:o:sgi:irix:6.5.9:*****:
cpe:2.3:a:sun:linux:5.0.7:*****:
cpe:2.3:a:sun:linux:5.0.7:*****:
cpe:2.3:o:sun:solaris:8.0:*:x86:*****:
cpe:2.3:o:sun:solaris:9.0:*:sparc:*****:
cpe:2.3:o:sun:solaris:9.0:*:x86:*****:
cpe:2.3:o:sun:solaris:8.0:*:x86:*****:
cpe:2.3:o:sun:solaris:9.0:*:sparc:*****:
cpe:2.3:o:sun:solaris:9.0:*:x86:*****:
cpe:2.3:o:sun:sunos:5.8:*****:
cpe:2.3:o:sun:sunos:5.8:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)