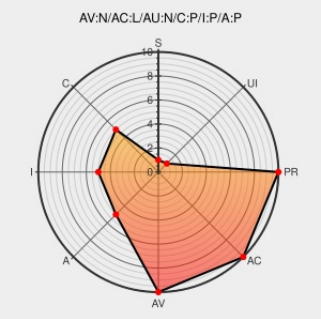
CVE-2010-1168

Published on: 06/21/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:18 AM UTC

CVE-2010-1168

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Perl from Perl contain the following vulnerability:

The Safe (aka Safe.pm) module before 2.25 for Perl allows context-dependent attackers to bypass intended (1) Safe::reval and (2) Safe::rdo access restrictions, and inject and execute arbitrary code, via vectors involving implicitly called methods and implicitly blessed objects, as demonstrated by the (a) DESTROY and (b) AUTOLOAD methods, related to "automagic methods."

CVE-2010-1168 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Red Hat Customer Portal	Vendor Advisory, www.redhat.com, text/html	REDHAT RHSA-2010:0458
2016-04 Security Bulletin: CTP Series: Multiple vulnerabilities in CTP Series - Juniper Networks	kb.juniper.net, text/html	CONFIRM kb.juniper.net/InfoCenter/index?page=content&id=JSA10735
Oracle Solaris Perl Safe Module Security Bypass - Advisories - Community	web.archive.org, text/html	SECUNIA 42402
SecurityTracker.com Archives - Perl Safe Module (Safe::reval and Safe::rdo) Can Be Bypassed	Vendor Advisory, securitytracker.com, text/html	SECTRACK 1024062

Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:9807
Red Hat update for perl - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 40049
oss-security - CVE-2010-1974 reject request (dupe of CVE-2010-1168) and CVE-2010-1447 description modification request	www.openwall.com text/html	MLIST [oss-security] 20100520 CVE-2010-1974 reject request (dupe of CVE-2010-1168) and CVE-2010-1447 description modification request
Red Hat update for perl - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 40052
Security	web.archive.org text/html Inactive Link Not Archived	CONFIRM blogs.sun.com/security/entry/cve_2010_1168_vulnerability_in
	cpansearch.perl.org text/plain	CONFIRM cpansearch.perl.org/src/RGARCIA/Safe-2.27/Changes
mandriva.com	www.mandriva.com text/html	MANDRIVA MDVSA-2010:115
Red Hat Customer Portal	Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2010:0457
mandriva.com	www.mandriva.com text/html	MANDRIVA MDVSA-2010:116
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2010-3075
Bug 576508 – CVE-2010-1168 perl Safe: Intended restriction bypass via object references	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=576508
Rafaël Garcia-Suarez at blog.perls.org: New Safe.pm fixes security hole	blogs.perl.org text/html	CONFIRM blogs.perl.org/users/rafael_garcia-suarez/2010/03/new-safepm-fixes-security-hole.html
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:7424
Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView	kb.juniper.net text/html	CONFIRM kb.juniper.net/InfoCenter/index?page=content&id=JSA10705

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Perl	Perl	All	All	All	All
Application	Perl	Perl	All	All	All	All
Application	Rafael Garcia-suarez	Safe	2.08	All	All	All

Application	Rafael Garcia-suarez	Safe	2.09	All	All	All
Application	Rafael Garcia-suarez	Safe	2.11	All	All	All
Application	Rafael Garcia-suarez	Safe	2.13	All	All	All
Application	Rafael Garcia-suarez	Safe	2.14	All	All	All
Application	Rafael Garcia-suarez	Safe	2.15	All	All	All
Application	Rafael Garcia-suarez	Safe	2.16	All	All	All
Application	Rafael Garcia-suarez	Safe	2.17	All	All	All
Application	Rafael Garcia-suarez	Safe	2.18	All	All	All
Application	Rafael Garcia-suarez	Safe	2.19	All	All	All
Application	Rafael Garcia-suarez	Safe	2.20	All	All	All
Application	Rafael Garcia-suarez	Safe	2.21	All	All	All
Application	Rafael Garcia-suarez	Safe	2.22	All	All	All
Application	Rafael Garcia-suarez	Safe	2.23	All	All	All
Application	Rafael Garcia-suarez	Safe	2.24	All	All	All
Application	Rafael Garcia-suarez	Safe	2.08	All	All	All
Application	Rafael Garcia-suarez	Safe	2.09	All	All	All
Application	Rafael Garcia-suarez	Safe	2.11	All	All	All
Application	Rafael Garcia-suarez	Safe	2.13	All	All	All
Application	Rafael Garcia-suarez	Safe	2.14	All	All	All
Application	Rafael Garcia-suarez	Safe	2.15	All	All	All
Application	Rafael Garcia-suarez	Safe	2.16	All	All	All
Application	Rafael Garcia-suarez	Safe	2.17	All	All	All
Application	Rafael Garcia-suarez	Safe	2.18	All	All	All
Application	Rafael Garcia-suarez	Safe	2.19	All	All	All
Application	Rafael Garcia-suarez	Safe	2.20	All	All	All
Application	Rafael Garcia-suarez	Safe	2.21	All	All	All
Application	Rafael Garcia-suarez	Safe	2.22	All	All	All
Application	Rafael Garcia-suarez	Safe	2.23	All	All	All
Application	Rafael Garcia-suarez	Safe	2.24	All	All	All

cpe:2.3:a:perl:perl:*:*:*:*:*:*:*:*:

cpe:2.3:a:perl:perl:*:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.08:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.09:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.11:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.13:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.14:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.15:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.16:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.17:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.18:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.19:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.20:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.21:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.22:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.23:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.24:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.08:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.09:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.11:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.13:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.14:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.15:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.16:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.17:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.18:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.19:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.20:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.21:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.22:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.23:*:*:*:*:*:*:*:

cpe:2.3:a:rafael_garcia-suarez:safe:2.24:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→