



CVE-2005-3962

Published on: 12/01/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:42 AM UTC

CVE-2005-3962

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

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

Integer overflow in the format string functionality (Perl_sv_vcatpvfn) in Perl 5.9.2 and 5.8.6 Perl allows attackers to overwrite arbitrary memory and possibly execute arbitrary code via format string specifiers with large values, which causes an integer wrap and leads to a buffer overflow, as demonstrated using format string vulnerabilities in Perl applications.

CVE-2005-3962 has been assigned by secalert@redhat.com 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

Repository / Oval Repository

[oval.cisecurity.org](#)
[text/html](#)

OVAL [oval.org.mitre.oval:def:10598](#)

Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia

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

SECUNIA 23155

Advisories - Mandriva Linux

[www.mandriva.com](#)
[text/html](#)

MANDRAKE MDKSA-2005:225

Security Announcement

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

SUSE SUSE-SA:2005:071

OpenBSD 3.7 errata

[www.openbsd.org](#)

OPENBSD [3.7] 20060105 007: SECURITY FIX: January 5, 2006

	text/html	2006
Perl Perl_sv_vcatpvfn Format String Integer Wrap Vulnerability	cve.report (archive) text/html	 BID 15629
[FLSA-2006:176731] Updated perl packages fix security issue	www.redhat.com text/html	 FEDORA FLSA-2006:176731
US-CERT Technical Cyber Security Alert TA06-333A -- Apple Releases Security Update to Address Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/html	 CERT TA06-333A
Secunia - Advisories - Red Hat update perl	Vendor Advisory web.archive.org text/html	 SECUNIA 18075
Secunia - Advisories - SUSE update for perl	Vendor Advisory web.archive.org text/html	 SECUNIA 18183
1. Overview:	support.avaya.com text/html	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-081.htm
Ubuntu update for perl - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 17762
#102192: Integer Overflow Vulnerability in Perl May Lead to Application Crash or Code Execution	web.archive.org text/html Inactive Link Not Archived	 SUNALERT 102192
Secunia - Advisories - Sun Solaris update for Perl	Vendor Advisory web.archive.org text/html	 SECUNIA 19041
Secunia - Advisories - Red Hat update for perl	Vendor Advisory web.archive.org text/html	 SECUNIA 18187
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2006-2613
'[Full-disclosure] Perl format string integer wrap vulnerability' - MARC	marc.info text/html	 FULLDISC 20051201 Perl format string integer wrap vulnerability
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20051201 Perl format string integer wrap vulnerability
SecurityFocus	www.securityfocus.com text/html	 HP HPSBTU02125
APPLE-SA-2006-11-28 Security Update 2006-007	lists.apple.com text/html	 APPLE APPLE-SA-2006-11-28
Secunia - Advisories - Gentoo update for perl	Vendor Advisory web.archive.org text/html	 SECUNIA 17941
US-CERT Vulnerability Note VU#948385	US Government Resource www.kb.cert.org text/html	 CERT-VN VU#948385
No Description Provided	patches.sgi.com Inactive Link Not Archived	 SGI 20060101-01-U
Secunia - Advisories - Mandriva update	Vendor Advisory	 SECUNIA 17952

Secunia - Advisories - mandriva update for perl	Vendor Advisory web.archive.org text/html	 SECUNIA 1732
rhn.redhat.com Red Hat Support	Vendor Advisory www.redhat.com text/html	 REDHAT RHSA-2005:880
Gentoo Linux Documentation -- Perl: Format string errors can lead to code execution	www.gentoo.org text/html	 GENTOO GLSA-200512-01
	www.trustix.org text/plain Inactive Link Not Archived	 TRUSTIX TSLSA-2005-0070
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates	Vendor Advisory web.archive.org text/html	 SECUNIA 18517
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 21345
IPCop update for perl - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 31208
Security Announcement	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SR:2005:029
	ftp.openbsd.org text/x-diff Inactive Link Not Archived	 CONFIRM ftp.openbsd.org/pub/OpenBSD/patches/3.7/common/007_perl.patch
OpenPKG: Security Advisory [OpenPKG-SA-2005.025-perl]	www.openpkg.org text/html	 OPENPKG OpenPKG-SA-2005.025
rhn.redhat.com Red Hat Support	Vendor Advisory www.redhat.com text/html	 REDHAT RHSA-2005:881
	ftp.openbsd.org text/x-diff Inactive Link Not Archived	 CONFIRM ftp.openbsd.org/pub/OpenBSD/patches/3.8/common/001_perl.patch
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:1074
IPCop 1.4.21 released :: IPCop.org :: The bad packets stop here!	www.ipcop.org text/html	 CONFIRM www.ipcop.org/index.php?name=News&file=article&sid=41
Secunia - Advisories - Debian update for perl	Vendor Advisory web.archive.org text/html	 SECUNIA 18413
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 22255
About the security content of Security Update 2006-007	web.archive.org text/html Inactive Link Not Archived	 CONFIRM docs.info.apple.com/article.html?artnum=304829
404: Not Found	Patch Vendor Advisory web.archive.org text/html	 MISC www.dyadsecurity.com/perl-0002.html

	text/html Inactive Link Not Archived	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2005-2688
USN-222-1: Perl vulnerability Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-222-1
Secunia - Advisories - Perl Explicit Format Parameter Index Integer Overflow Vulnerability	Vendor Advisory web.archive.org text/html	 SECUNIA 17802
Secunia - Advisories - Trustix update for perl	Vendor Advisory web.archive.org text/html	 SECUNIA 17993
Secunia - Advisories - OpenBSD update for perl	Vendor Advisory web.archive.org text/html	 SECUNIA 18295
Secunia - Advisories - HP Tru64 UNIX and HP Internet Express Perl Vulnerability	Vendor Advisory web.archive.org text/html	 SECUNIA 20894
Home - Conectiva	distro.conectiva.com.br text/html	 CONECTIVA CLSA-2006:1056
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2006-0771
Fedora update for perl - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 17844
Debian -- Security Information -- DSA-943-1 perl	www.debian.org Deprecated Link text/html	 DEBIAN DSA-943
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2006-4750

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
Application	Perl	Perl	5.8.6	All	All	All
Application	Perl	Perl	5.9.2	All	All	All
Application	Perl	Perl	5.8.6	All	All	All
Application	Perl	Perl	5.9.2	All	All	All
cpe:2.3:a:perl:perl:5.8.6:*:*:*:*:*:						
cpe:2.3:a:perl:perl:5.9.2:*:*:*:*:*:						

cpe:2.3:a:perl:perl:5.8.6:*****:

cpe:2.3:a:perl:perl:5.9.2:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2023  |

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](#)