CVE-2011-1938

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2011-1938
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-31 20:55:00 UTC
Updated	2017-08-17 01:34:00 UTC
Description	Stack-based buffer overflow in the socket_connect function in ext/sockets/sockets.c in PHP 5.3.3 through 5.3.6 might allow

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	5.3.3	All	All	All
Application	Php	Php	5.3.4	All	All	All
Application	Php	Php	5.3.5	All	All	All
Application	Php	Php	5.3.6	All	All	All
Application	Php	Php	5.3.3	All	All	All
Application	Php	Php	5.3.4	All	All	All
Application	Php	Php	5.3.5	All	All	All
Application	Php	Php	5.3.6	All	All	All

References

Reference	Source	L
APPLE-SA-2012-02-01-1 OS X Lion v10.7.3 and Security Update 2012-001	APPLE	li
Security Advisories | Mandriva Linux	MANDRIVA	w
PHP: Diff of /php/php-src/trunk/ext/sockets/sockets.c	CONFIRM	s
oss-security - CVE request: PHP socket_connect() - stack buffer overflow	MLIST	o
72644	OSVDB	o
Malformed Request	BID	w

'[security bulletin] HPSBOV02763 SSRT100826 rev.1 - HP Secure Web Server (SWS) for OpenVMS running PH' - MARC	HP	n
PHP: News Archive - 2011	CONFIRM	w
PHP: Revision 311369	CONFIRM	s
PHP <= 5.3.5 socket_connect() Buffer Overflow Vulnerability - SecurityReason.com	SREASON	s
About the security content of OS X Lion v10.7.3 and Security Update 2012-001	CONFIRM	s
Debian -- Security Information -- DSA-2399-2 php5	DEBIAN	w
oss-security - Re: CVE request: PHP socket_connect() - stack buffer overflow	MLIST	o
PHP <= 5.3.5 socket_connect() Buffer Overflow Vulnerability	EXPLOIT-DB	w
IBM X-Force Exchange	XF	e
access.redhat.com	REDHAT	w
PHP: PHP 5 ChangeLog	CONFIRM	w
PHP 5.3.6 Buffer Overflow PoC (ROP) CVE-2011-1938 - SecurityReason.com	SREASON	s
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**