

CVE Details

The ultimate security vulnerability datasource

Log In

Register

Reset Password

Activate Account

Vulnerability Feeds & Widgets^{New}

www.itsecdb.com

Home

Browse :

Vendors

Products

Vulnerabilities By Date

Vulnerabilities By Type

Reports :

CVSS Score Report

CVSS Score Distribution

Search :

Vendor Search

Product Search

Version Search

Vulnerability Search

By Microsoft References

Top 50 :

Vendors

Vendor Cvss Scores

Products

Product Cvss Scores

Versions

Other :

Microsoft Bulletins

Bugtraq Entries

CWE Definitions

About & Contact

Feedback

CVE Help

FAQ

Articles

External Links :

NVD Website

CWE Web Site

View CVE :

Go

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :

Go

(e.g.: 12345)

Search By Microsoft Reference ID:

Go

(e.g.: ms10-001 or 979352)

Vulnerability Details : CVE-2013-2765

The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

Publish Date : 2013-07-15 Last Update Date : 2013-11-18

Collapse All

Expand All

Select

Select&Copy

Scroll To

Comments

External Links

Search Twitter

Search YouTube

Search Google

– CVSS Scores & Vulnerability Types

CVSS Score4.3

Confidentiality ImpactNone (There is no impact to the confidentiality of the system.)

Integrity ImpactNone (There is no impact to the integrity of the system)

Availability ImpactPartial (There is reduced performance or interruptions in resource availability.)

Access ComplexityMedium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)

AuthenticationNot required (Authentication is not required to exploit the vulnerability.)

Gained AccessNone

Vulnerability Type(s)Denial Of Service

CWE IDCWE id is not defined for this vulnerability

– Products Affected By CVE-2013-2765

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Modsecurity	Modsecurity	2.7.0				Version Details Vulnerabilities
2	Application	Modsecurity	Modsecurity	2.7.0	RC3			Version Details Vulnerabilities
3	Application	Modsecurity	Modsecurity	2.7.1				Version Details Vulnerabilities
4	Application	Modsecurity	Modsecurity	2.7.2				Version Details Vulnerabilities
5	Application	Modsecurity	Modsecurity	2.7.3				Version Details Vulnerabilities

– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Modsecurity	Modsecurity	5

– References For CVE-2013-2765

<http://archives.neohapsis.com/archives/bugtraq/2013-05/0125.html>
BUGTRAQ 20130528 [SECURITY][CVE-2013-2765][ModSecurity] Remote Null Pointer Dereference

<http://lists.opensuse.org/opensuse-updates/2013-08/msg00020.html>
SUSE openSUSE-SU-2013:1331

<http://lists.opensuse.org/opensuse-updates/2013-08/msg00025.html>
SUSE openSUSE-SU-2013:1336

<http://lists.opensuse.org/opensuse-updates/2013-08/msg00031.html>
SUSE openSUSE-SU-2013:1342

http://sourceforge.net/mailarchive/message.php?msg_id=30900019
MLIST [mod-security-users] 20130527 Availability of ModSecurity 2.7.4 Stable Release

WIZ, Inc. EXHIBIT - 1103 - WIZ, Inc. v. Orca Security LTD.

https://bugzilla.redhat.com/show_bug.cgi?id=967615 CONFIRM

<http://www.shookalabs.com/>

<http://www.modsecurity.org/> CONFIRM

<https://raw.githubusercontent.com/SpiderLabs/ModSecurity/master/CHANGES> CONFIRM

<https://github.com/SpiderLabs/ModSecurity/commit/0840b13612a0b7ef1ce7441cf811dcfc6b463fba>

https://github.com/shookalabs/exploits/blob/master/modsecurity_cve_2013_2765_check.py

– Vulnerability Conditions

Vulnerability is valid if product versions listed below are used **TOGETHER WITH**(AND)

- [Modsecurity Modsecurity 2.7.0 RC3](#)
- [Modsecurity Modsecurity 2.7.0](#)
- [Modsecurity Modsecurity 2.7.2](#)
- [Modsecurity Modsecurity 2.7.1](#)
- [Modsecurity Modsecurity 2.7.3](#)
- [Apache Http Server](#)

– Metasploit Modules Related To CVE-2013-2765

There are not any metasploit modules related to this vulnerability (Please visit www.metasploit.com for more information)

[How does it work?](#) [Known limitations & technical details](#) [User agreement, disclaimer and privacy statement](#) [About & Contact](#) [Feedback](#)

CVE is a registered trademark of the MITRE Corporation and the authoritative source of CVE content is [MITRE's CVE web site](#). CWE is a registered trademark of the MITRE Corporation and the authoritative source of CWE content is [MITRE's CWE web site](#). OVAL is a registered trademark of The MITRE Corporation and the authoritative source of OVAL content is [MITRE's OVAL web site](#).

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.