CVE-2007-0911

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

Summary

CVE	CVE-2007-0911
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-02-13 23:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Off-by-one error in the str_ireplace function in PHP 5.2.1 might allow context-dependent attackers to cause a denial of servi

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:C

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:N/AC:L/Au:N/C:N/I:N/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	5.2.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Sou
SUSE update for php4 and php5 - Advisories - Secunia	af85
'[PHP-DEV] PHP 5.2.1 crashing Apache/IIS...' - MARC	af85
'Re: [PHP-DEV] PHP 5.2.1 crashing Apache/IIS...' - MARC	af85
Gentoo update for php - Advisories - Secunia	af85
cvs.php.net/viewvc.cgi/php-src/ext/standard/string.c	af85
PHP STR_IReplace Remote Denial of Service Vulnerability	af85
SecurityFocus	af85
osvdb.org/33952	af85
Gentoo Linux Documentation -- PHP: Multiple vulnerabilities	af85
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: php security problems (SUSE-SA:2007:020)	af85
CVE Program record	CVE
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-02-16	Mark J Cox	Not vulnerable. This flaw is a regression of the fix for CVE-2007-0906 affecting PHP version 5.2.

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