CVE-2008-1066

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

Summary

CVE	CVE-2008-1066
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-02-28 20:44:00 UTC
Updated	2017-08-08 01:29:00 UTC
Description	The modifier.regex_replace.php plugin in Smarty before 2.6.19, as used by Serendipity (S9Y) and other products, allows at

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Smarty	Smarty	All	All	All	All

References

Reference	Source	Lin
Smarty :: View topic - Smarty 2.6.19 Released	CONFIRM	ww
Fedora update for gallery2 - Advisories - Secunia	SECUNIA	sec
Smarty Template Engine 'regex_replace' Template Security Bypass Vulnerability	BID	ww
[security-announce] SUSE Security Summary Report SUSE-SR:2008:007	SUSE	lists
IBM X-Force Exchange	XF	exc
Fedora update for php-pear-PhpDocumentor - Advisories - Secunia	SECUNIA	sec
Smarty "regex_replace" Modifier Template Security Bypass - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	sec
[SECURITY] Fedora 8 Update: gallery2-2.2.4-3.fc8	FEDORA	ww
SUSE Update for Multiple Packages - Advisories - Secunia	SECUNIA	sec
Debian update for smarty - Advisories - Secunia	SECUNIA	sec
Serendipity 1.3-beta1 released - Serendipity	CONFIRM	blo
[SECURITY] Fedora 7 Update: gallery2-2.2.4-3.fc7	FEDORA	ww
Gentoo Linux Documentation -- phpDocumentor: Function call injection	GENTOO	sec

Debian -- Security Information -- DSA-1520-1 smarty	DEBIAN	ww
Serendipity Security Bypass and Script Insertion Vulnerabilities - Advisories - Secunia	SECUNIA	sec
Search Results for "misc" | Smarty	CONFIRM	ww
[SECURITY] Fedora 8 Update: php-pear-PhpDocumentor-1.4.1-2.fc8	FEDORA	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

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**