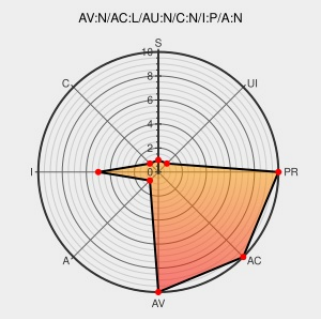
CVE-2004-1620

Published on: 10/21/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1620

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Serendipity from S9y contain the following vulnerability:

CRLF injection vulnerability in Serendipity before 0.7rc1 allows remote attackers to perform HTTP Response Splitting attacks to modify expected HTML content from the server via the url parameter in (1) index.php and (2) exit.php, or (3) the HTTP Referer field in comment.php.

CVE-2004-1620 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Secunia - Advisories - Serendipity Unspecified HTTP Response Splitting Vulnerability	Exploit, Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 12909
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF serendipity-response-splitting(17798)
No Description Provided	cvs.sourceforge.net, Inactive Link, Not Archived	CONFIRM cvs.sourceforge.net/viewcvs.py/php-blog/serendipity/comment.php?rev=1.49&view=markup
No Description Provided	www.osvdb.org	OSVDB 11039

	Inactive Link Not Archived	
'HTTP Response Splitting in Serendipity 0.7-beta4' - MARC	marc.info text/html	BUGTRAQ 20041021 HTTP Response Splitting in Serendipity 0.7-beta4
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 11013
No Description Provided	cvs.sourceforge.net Inactive Link Not Archived	CONFIRM cvs.sourceforge.net/viewcvs.py/php-blog/serendipity/index.php?rev=1.52&view=markup
SecurityTracker.com Archives - Serendipity Input Validation Flaws in Processing Request URI and HTTP Referer Field May Permit HTTP Response Splitting Attacks	securitytracker.com text/html	SECTRACK 1011864
SourceForge.net: File Release Notes and Changelog	web.archive.org text/html Inactive Link Not Archived	CONFIRM sourceforge.net/project/shownotes.php?release_id=276694
Serendipity - A reliable, secure and extensible PHP blog | Serendipity Blog System	Exploit Patch Vendor Advisory www.s9y.org text/html	CONFIRM www.s9y.org/5.html
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 11038
No Description Provided	cvs.sourceforge.net Inactive Link Not Archived	CONFIRM cvs.sourceforge.net/viewcvs.py/php-blog/serendipity/exit.php?rev=1.10&view=markup
Serendipity Exit.PHP HTTP Response Splitting Vulnerability	Exploit Patch Vendor Advisory cve.report (archive) text/html	BID 11497

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	S9y	Serendipity	0.3	All	All	All
Application	S9y	Serendipity	0.4	All	All	All
Application	S9y	Serendipity	0.5	All	All	All
Application	S9y	Serendipity	0.5_pl1	All	All	All

Application	S9y	Serendipity	0.6	All	All	All
Application	S9y	Serendipity	0.6_pl1	All	All	All
Application	S9y	Serendipity	0.6_pl2	All	All	All
Application	S9y	Serendipity	0.6_pl3	All	All	All
Application	S9y	Serendipity	0.6_rc1	All	All	All
Application	S9y	Serendipity	0.6_rc2	All	All	All
Application	S9y	Serendipity	0.7_beta1	All	All	All
Application	S9y	Serendipity	0.7_beta2	All	All	All
Application	S9y	Serendipity	0.7_beta3	All	All	All
Application	S9y	Serendipity	0.7_beta4	All	All	All
Application	S9y	Serendipity	0.3	All	All	All
Application	S9y	Serendipity	0.4	All	All	All
Application	S9y	Serendipity	0.5	All	All	All
Application	S9y	Serendipity	0.5_pl1	All	All	All
Application	S9y	Serendipity	0.6	All	All	All
Application	S9y	Serendipity	0.6_pl1	All	All	All
Application	S9y	Serendipity	0.6_pl2	All	All	All
Application	S9y	Serendipity	0.6_pl3	All	All	All
Application	S9y	Serendipity	0.6_rc1	All	All	All
Application	S9y	Serendipity	0.6_rc2	All	All	All
Application	S9y	Serendipity	0.7_beta1	All	All	All
Application	S9y	Serendipity	0.7_beta2	All	All	All
Application	S9y	Serendipity	0.7_beta3	All	All	All
Application	S9y	Serendipity	0.7_beta4	All	All	All

cpe:2.3:a:s9y:serendipity:0.3:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.4:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.5:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.5_pl1:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.6:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.6_pl1:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.6_pl2:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.6_pl3:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.6_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.6_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.7_beta1:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.7_beta2:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.7_beta3:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.7_beta4:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.3:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.4:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.5:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.5_pl1:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.6:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.6_pl1:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.6_pl2:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.6_pl3:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.6_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.6_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.7_beta1:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.7_beta2:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.7_beta3:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.7_beta4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→