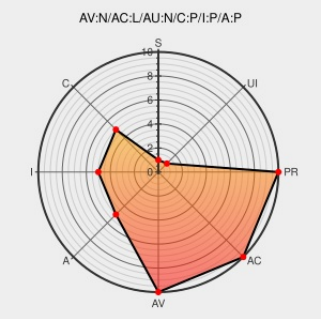
CVE-2005-1451

Published on: 05/03/2005 12:00:00 AM UTC

Last Modified on: 06/15/2021 12:00:00 AM UTC

CVE-2005-1451

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



Certain versions of Serendipity from S9y contain the following vulnerability:

The media manager in Serendipity before 0.8 allows remote attackers to upload and execute arbitrary (1) .php or (2) .shtml files.

CVE-2005-1451 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Secunia - Advisories - Serendipity Multiple Vulnerabilities	Patch, web.archive.org, text/html	SECUNIA 15145
404 Not Found	Patch, web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM www.s9y.org/63.html#A9
No Description Provided	www.osvdb.org, Inactive Link, Not Archived	OSVDB 15878

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_pl1	All	All	All
Application	S9y	Serendipity	0.6_pl3	All	All	All
Application	S9y	Serendipity	0.7	All	All	All
Application	S9y	Serendipity	0.7.1	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	0.7_rc1	All	All	All
Application	S9y	Serendipity	0.8_beta_5	All	All	All
Application	S9y	Serendipity	0.8_beta_6	All	All	All
Application	S9y	Serendipity	0.3	All	All	All
Application	S9y	Serendipity	0.4	All	All	All
Application	S9y	Serendipity	0.5_pl1	All	All	All
Application	S9y	Serendipity	0.6_pl3	All	All	All
Application	S9y	Serendipity	0.7	All	All	All
Application	S9y	Serendipity	0.7.1	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	0.7_rc1	All	All	All
Application	S9y	Serendipity	0.8_beta_5	All	All	All
Application	S9y	Serendipity	0.8_beta_6	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_pl1:*:*:*:*:*:*:*:

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

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

cpe:2.3:a:s9y:serendipity:0.7.1:*:*:*:*:*:*:*:

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:0.7_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.8_beta_5:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.8_beta_6:*:*:*:*:*:*:*:

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

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

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

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

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

cpe:2.3:a:s9y:serendipity:0.7.1:*:*:*:*:*:*:*:

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:0.7_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.8_beta_5:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.8_beta_6:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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