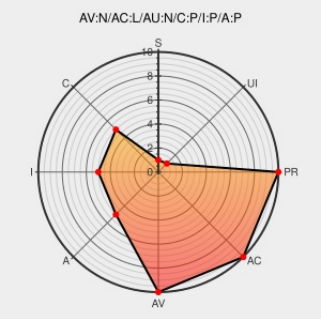
CVE-2005-1134

Published on: 04/13/2005 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1134

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



Certain versions of Serendipity from S9y contain the following vulnerability:

SQL injection vulnerability in exit.php for Serendipity 0.8 and earlier allows remote attackers to execute arbitrary SQL commands via the (1) url_id or (2) entry_id parameters.

CVE-2005-1134 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, Vendor Advisory, web.archive.org, text/html	SECUNIA 15145
Bugtraq: serendipity SQL Injection vulnerability	seclists.org, text/html	BUGTRAQ 20050413 serendipity SQL Injection vulnerability
404 Not Found	Patch, Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM www.s9y.org/63.html#A9
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF serendipity-urlid-entryid-sql-injection(20119)

No Description Provided	Vendor Advisory www.osvdb.org Inactive Link Not Archived	OSVDB 15542
Serendipity - A reliable, secure and extensible PHP blog | Serendipity Blog System	Patch Vendor Advisory www.s9y.org text/html	CONFIRM www.s9y.org/5.html
S9Y Serendipity Exit.PHP SQL injection Vulnerability	Exploit Patch Vendor Advisory cve.report (archive) text/html	BID 13161
Serendipity Input Validation Error in 'exit.php' Permits SQL Injection Attacks - SecurityTracker	Vendor Advisory securitytracker.com text/html	SECTRACK 1013699

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	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_beta5	All	All	All

Application	S9y	Serendipity	0.8_beta6	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	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_beta5	All	All	All
Application	S9y	Serendipity	0.8_beta6	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:*:*:*:*:*:*:*:

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_beta5:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.8_beta6:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:

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_beta5:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:0.8_beta6:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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