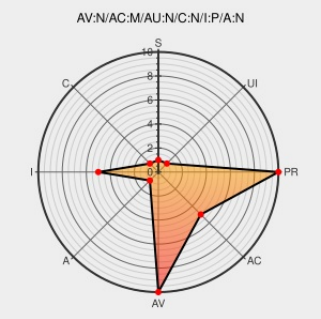
CVE-2005-4454

Published on: 12/21/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-4454

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



Certain versions of Livejournal from Livejournal contain the following vulnerability:

Validate-before-filter vulnerability in cleanhtml.pl 1.129 in LiveJournal CVS before Dec 7 2005, when the cleancss option is enabled, allows remote attackers to conduct cross-site scripting (XSS) attacks via a "\" (backslash) within a "javascript" scheme in a style property (such as "javas\cript"), which bypasses the "javascript" check before the "\" is stripped and then rendered in web browsers that allow scripting in style sheets.

CVE-2005-4454 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF livejournal-javascript-xss(23839)
Secunia - Advisories - LiveJournal "cleanhtml.pl" Two Script Insertion Vulnerabilities	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18157
LiveJournal Cleanhtml.PL HTML Injection Vulnerability	Exploit cve.report (archive) text/html	BID 15990
No Description Provided	web.archive.org text/html	FULLDISC 20051219 LiveJournal CSS/JS injection vulnerability

	Inactive Link Not Archived	injection vulnerability
CVS log for livejournal/cgi-bin/cleanhtml.pl	cvs.livejournal.org text/html	CONFIRM cvs.livejournal.org/browse.cgi/livejournal/cgi-bin/cleanhtml.pl
'[Full-disclosure] LiveJournal CSS/JS injection vulnerability' - MARC	marc.info text/html	FULLDISC 20051220 LiveJournal CSS/JS injection vulnerability
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 21896

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:livejournal:livejournal:*:*:*:*:*:*:*:*:

cpe:2.3:a:livejournal:livejournal:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→