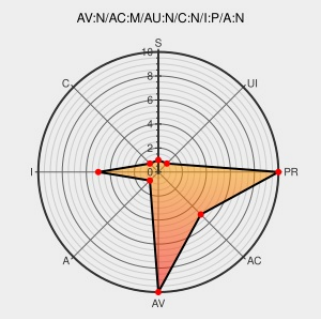
CVE-2010-2013

Published on: 05/24/2010 12:00:00 AM UTC

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

CVE-2010-2013

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



Certain versions of Lisk Cms from Createch-group contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in cp/edit_email.php in LiSK CMS 4.4 allows remote attackers to inject arbitrary web script or HTML via the id parameter.

CVE-2010-2013 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
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20100520 XSS vulnerability in LiSK CMS
Lisk CMS Cross-Site Scripting and SQL Injection Vulnerabilities - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 39912
High-Tech Bridge SA - Advisories - XSS vulnerability in LiSK CMS	Exploit web.archive.org text/html Inactive Link Not Archived	MISC www.htbridge.ch/advisory/xss_vulnerability_in_product.html

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	Createch-group	Lisk Cms	4.4	All	All	All
Application	Createch-group	Lisk Cms	4.4	-	corporate	All
Application	Createch-group	Lisk Cms	4.4	-	custom	All
Application	Createch-group	Lisk Cms	4.4	-	e-commerce	All
Application	Createch-group	Lisk Cms	4.4	-	extranet/intranet	All
Application	Createch-group	Lisk Cms	4.4	-	extranet\/intranet	All
Application	Createch-group	Lisk Cms	4.4	-	portal/community	All
Application	Createch-group	Lisk Cms	4.4	-	portal\/community	All
Application	Createch-group	Lisk Cms	4.4	All	All	All
Application	Createch-group	Lisk Cms	4.4	-	corporate	All
Application	Createch-group	Lisk Cms	4.4	-	custom	All
Application	Createch-group	Lisk Cms	4.4	-	e-commerce	All
Application	Createch-group	Lisk Cms	4.4	-	extranet\/intranet	All
Application	Createch-group	Lisk Cms	4.4	-	portal\/community	All

cpe:2.3:a:createch-group:lisk_cms:4.4:*:*:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:-:corporate:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:-:custom:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:-:e-commerce:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:-:extranet/intranet:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:-:extranet\/intranet:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:-:portal/community:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:-:portal\/community:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:*:*:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:-:corporate:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:-:custom:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:-:e-commerce:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:-:extranet\/intranet:*:*:*:*:*:

cpe:2.3:a:createch-group:lisk_cms:4.4:-:portal\/community:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→