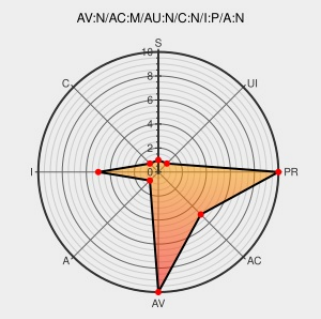
CVE-2004-1412

Published on: 12/31/2004 05:00:00 AM UTC

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

CVE-2004-1412

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



Certain versions of Esupport from Kayako contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in index.php in Kayako eSupport 2.x allows remote attackers to inject arbitrary web script or HTML via the searchm parameter.

CVE-2004-1412 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
Kayako ESupport Multiple Cross-Site Scripting and SQL Injection Vulnerabilities	Exploit, cve.report (archive), text/html	BID 12037
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF kayako-index-xss(18571)
'Multiple Vulnerabilities In Kayako eSupport v2.x' - MARC	marc.info, text/html	BUGTRAQ 20041218 Multiple Vulnerabilities In Kayako eSupport v2.x
Contact Support	Exploit, www.gulftech.org, text/html	MISC www.gulftech.org/?node=research&article_id=00056-12182004

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	Kayako	Esupport	2.1.2	All	All	All
Application	Kayako	Esupport	2.1.8	All	All	All
Application	Kayako	Esupport	2.2	All	All	All
Application	Kayako	Esupport	2.2.5	All	All	All
Application	Kayako	Esupport	2.3	All	All	All
Application	Kayako	Esupport	2.1.2	All	All	All
Application	Kayako	Esupport	2.1.8	All	All	All
Application	Kayako	Esupport	2.2	All	All	All
Application	Kayako	Esupport	2.2.5	All	All	All
Application	Kayako	Esupport	2.3	All	All	All

cpe:2.3:a:kayako:esupport:2.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:kayako:esupport:2.1.8:*:*:*:*:*:*:*:

cpe:2.3:a:kayako:esupport:2.2:*:*:*:*:*:*:*:

cpe:2.3:a:kayako:esupport:2.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:kayako:esupport:2.3:*:*:*:*:*:*:*:

cpe:2.3:a:kayako:esupport:2.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:kayako:esupport:2.1.8:*:*:*:*:*:*:*:

cpe:2.3:a:kayako:esupport:2.2:*:*:*:*:*:*:*:

cpe:2.3:a:kayako:esupport:2.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:kayako:esupport:2.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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