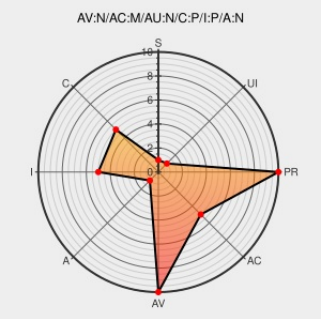
CVE-2006-2257

Published on: 05/09/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:08 PM UTC

CVE-2006-2257

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



Certain versions of Easyevent from Faktorystudios contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in index.php in easyEvent 1.2 allows remote attackers to inject arbitrary web script or HTML via the curr_year parameter.

CVE-2006-2257 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
EasyEvent "curr_year" Cross-Site Scripting Vulnerability - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 20038
FaktoryStudios EasyEvent Index.PHP Cross-Site Scripting Vulnerability	cve.report (archive), text/html	BID 17891
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF easyevent-index-xss(26332)
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com, text/html	VUPEN ADV-2006-1695
No Description Provided	www.osvdb.org	OSVDB 25341

	Inactive Link Not Archived	
SecurityTracker.com Archives - easyEvent Input Validation Hole in 'curr_year' Parameter Permits Cross-Site Scripting Attacks	securitytracker.com text/html	SECTRACK 1016105

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	Faktorystudios	Easyevent	1.0	All	All	All
Application	Faktorystudios	Easyevent	1.1	All	All	All
Application	Faktorystudios	Easyevent	1.2	All	All	All
Application	Faktorystudios	Easyevent	1.0	All	All	All
Application	Faktorystudios	Easyevent	1.1	All	All	All
Application	Faktorystudios	Easyevent	1.2	All	All	All

cpe:2.3:a:faktorystudios:easyevent:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:faktorystudios:easyevent:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:faktorystudios:easyevent:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:faktorystudios:easyevent:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:faktorystudios:easyevent:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:faktorystudios:easyevent:1.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→