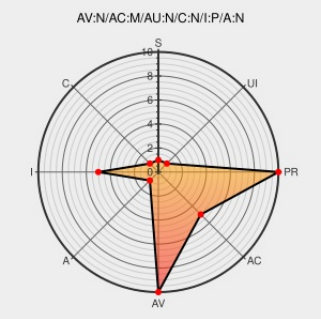
CVE-2014-8690

Published on: 02/19/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:50 PM UTC

CVE-2014-8690

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



Certain versions of Exponent Cms from Exponentcms contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in Exponent CMS before 2.1.4 patch 6, 2.2.x before 2.2.3 patch 9, and 2.3.x before 2.3.1 patch 4 allow remote attackers to inject arbitrary web script or HTML via the (1) PATH_INFO, the (2) src parameter in a none action to index.php, or the (3) "First Name" or (4) "Last Name" field to users/edituser.

CVE-2014-8690 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
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 118263
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF exponentcms-cve20148690-xss(100877)
Exponent CMS 2.3.1 - Multiple XSS Vulnerabilities	Exploit www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 36059
No Description Provided	osvdb.org	OSVDB 118345

	Inactive Link Not Archived	
Exponent CMS Multiple Input Validation Holes Permit Cross-Site Scripting Attacks - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1031775
#1230 Universal cross-site scripting in Exponent CMS 2.3.1 and prior - Exponent CMS - exponentcms	exponentcms.lighthouseapp.com text/html	CONFIRM exponentcms.lighthouseapp.com/projects/61783/tickets/1230-universal-cross-site-scripting-in-exponent-cms-231-and-prior
Exponent CMS 2.3.1 Cross Site Scripting ≈ Packet Storm	Exploit packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/130382/Exponent-CMS-2.3.1-Cross-Site-Scripting.html
Corrected Security Patches released for v2.1.4, v2.2.3, and v2.3.1	Patch Vendor Advisory www.exponentcms.org text/html	CONFIRM www.exponentcms.org/news/show/title/corrected-security-patches-released-for-v2-1-4-v2-2-3-and-v2-3-0

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Exponentcms	Exponent Cms	2.2.0	All	All	All
Application	Exponentcms	Exponent Cms	2.2.1	All	All	All
Application	Exponentcms	Exponent Cms	2.2.2	All	All	All
Application	Exponentcms	Exponent Cms	2.2.3	All	All	All
Application	Exponentcms	Exponent Cms	2.3.0	All	All	All
Application	Exponentcms	Exponent Cms	2.3.1	All	All	All
Application	Exponentcms	Exponent Cms	2.2.0	All	All	All
Application	Exponentcms	Exponent Cms	2.2.1	All	All	All
Application	Exponentcms	Exponent Cms	2.2.2	All	All	All
Application	Exponentcms	Exponent Cms	2.2.3	All	All	All
Application	Exponentcms	Exponent Cms	2.3.0	All	All	All
Application	Exponentcms	Exponent Cms	2.3.1	All	All	All
Application	Exponentcms	Exponent Cms	All	All	All	All

cpe:2.3:a:exponentcms:exponent_cms:2.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:exponentcms:exponent_cms:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:exponentcms:exponent_cms:2.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:exponentcms:exponent_cms:2.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:exponentcms:exponent_cms:2.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:exponentcms:exponent_cms:2.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:exponentcms:exponent_cms:2.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:exponentcms:exponent_cms:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:exponentcms:exponent_cms:2.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:exponentcms:exponent_cms:2.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:exponentcms:exponent_cms:2.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:exponentcms:exponent_cms:2.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:exponentcms:exponent_cms:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→