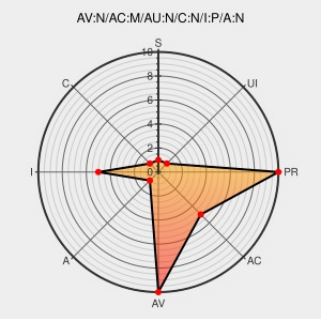
CVE-2013-2312

Published on: 05/29/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:43 PM UTC

CVE-2013-2312

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



Certain versions of Ec-cube from Lockon contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the shopping-cart screen in LOCKON EC-CUBE 2.11.0 through 2.12.3enP2 allows remote attackers to inject arbitrary web script or HTML via a crafted URL.

CVE-2013-2312 has been assigned by vultures@jpcert.or.jp 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
JVN#52552792: EC-CUBE vulnerable to cross-site scripting	jvn.jp, text/xml	JVN JVN#52552792
Changeset 22604 – EC-CUBE Trac	svn.ec-cube.net, text/html	CONFIRM svn.ec-cube.net/open_trac/changeset/22604
脆弱性 / 日本発!ECオープンプラットフォーム EC-CUBE	Vendor Advisory, www.ec-cube.net, text/xml	CONFIRM www.ec-cube.net/info/weakness/weakness.php?id=40
No Description Provided	jvndb.jvn.jp, text/html	JVNDB JVNDB-2013-000041

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	Lockon	Ec-cube	2.11.0	All	All	All
Application	Lockon	Ec-cube	2.11.1	All	All	All
Application	Lockon	Ec-cube	2.11.2	All	All	All
Application	Lockon	Ec-cube	2.11.3	All	All	All
Application	Lockon	Ec-cube	2.11.4	All	All	All
Application	Lockon	Ec-cube	2.11.5	All	All	All
Application	Lockon	Ec-cube	2.12.0	All	All	All
Application	Lockon	Ec-cube	2.12.1	All	All	All
Application	Lockon	Ec-cube	2.12.2	All	All	All
Application	Lockon	Ec-cube	2.12.3	All	All	All
Application	Lockon	Ec-cube	2.12.3en	All	All	All
Application	Lockon	Ec-cube	2.12.3enp1	All	All	All
Application	Lockon	Ec-cube	2.12.3enp2	All	All	All
Application	Lockon	Ec-cube	2.11.0	All	All	All
Application	Lockon	Ec-cube	2.11.1	All	All	All
Application	Lockon	Ec-cube	2.11.2	All	All	All
Application	Lockon	Ec-cube	2.11.3	All	All	All
Application	Lockon	Ec-cube	2.11.4	All	All	All
Application	Lockon	Ec-cube	2.11.5	All	All	All
Application	Lockon	Ec-cube	2.12.0	All	All	All
Application	Lockon	Ec-cube	2.12.1	All	All	All
Application	Lockon	Ec-cube	2.12.2	All	All	All
Application	Lockon	Ec-cube	2.12.3	All	All	All
Application	Lockon	Ec-cube	2.12.3en	All	All	All
Application	Lockon	Ec-cube	2.12.3enp1	All	All	All
Application	Lockon	Ec-cube	2.12.3enp2	All	All	All

cpe:2.3:a:lockon:ec-cube:2.11.0:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.11.1:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.11.2:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.11.3:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.11.4:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.11.5:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.0:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.1:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.2:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.3:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.3en:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.3enp1:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.3enp2:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.11.0:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.11.1:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.11.2:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.11.3:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.11.4:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.11.5:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.0:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.1:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.2:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.3:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.3en:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.3enp1:*:*:*:*:*:*:*:

cpe:2.3:a:lockon:ec-cube:2.12.3enp2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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