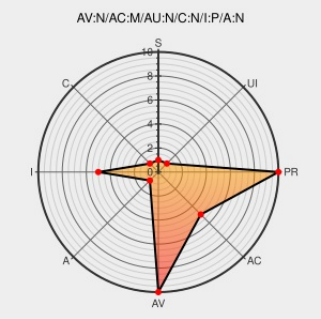
CVE-2012-6632

Published on: 01/16/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:22 PM UTC

CVE-2012-6632

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



Certain versions of Netbill from Vessio contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in Vessio NetBill 1.2 allow remote attackers to inject arbitrary web script or HTML via the (1) full name or (2) file title to accounts/admin/index.php or (3) comment parameter in the support page to accounts/index2.php.

CVE-2012-6632 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
NetBill Billing System 1.2 CSRF / XSS ≈ Packet Storm	Exploit, packetstormsecurity.org, text/html	MISC packetstormsecurity.org/files/112655/NetBill-Billing-System-1.2-CSRF-XSS.html
Security Alerts - Secunia	web.archive.org, text/html	SECUNIA 49109
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF netbill-index-xss(75538)
No Description Provided	www.osvdb.org, Inactive Link, Not Archived	OSVDB 81880
403 Forbidden	Exploit, www.vulnerability-lab.com, text/plain	MISC www.vulnerability-lab.com/get_content.php?id=560

Inactive Link Not Archived

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	Vessio	Netbill	1.2	All	All	All
Application	Vessio	Netbill	1.2	All	All	All

cpe:2.3:a:vessio:netbill:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:vessio:netbill:1.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→