



CVE-2012-6631

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

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

CVE-2012-6631

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Netbill** from **Vessio** contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in accounts/admin/index.php in Vessio NetBill 1.2 allows remote attackers to hijack the authentication of administrators for requests that add accounts via a new-client action.

CVE-2012-6631 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

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](http://MISC.packetstormsecurity.org/files/112655/NetBill-Billing-System-1.2-CSRF-XSS.html)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
text/html

[XF netbill-index-csrf\(75539\)](https://xforce.ibmcloud.com/exchange/view/75539)

No Description Provided

www.osvdb.org

[OSVDB 81881](https://osvdb.org/entry/view/81881)

Inactive Link **Not Archived**

Security Alerts - Secunia

web.archive.org
text/html

[SECUNIA 49109](https://secunia.com/advisories/49109)

403 Forbidden

Exploit
www.vulnerability-lab.com
text/plain

[MISC www.vulnerability-lab.com/get_content.php?id=560](http://MISC.www.vulnerability-lab.com/get_content.php?id=560)

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 →