



CVE-2012-3522

Published on: 06/13/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:17 PM UTC

CVE-2012-3522

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Geshi](#) from [Qbnz](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in contrib/langwiz.php in GeSHi before 1.0.8.11 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVE-2012-3522 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

[SECURITY] Fedora 17 Update: php-geshi-1.0.8.11-3.fc17

[lists.fedoraproject.org](https://lists.fedoraproject.org/text/html)
text/html

[FEDORA FEDORA-2013-5440](#)

oss-security - Re: CVE Request -- php-geshi / GeSHi (1.0.8.11): Remote directory traversal and information disclosure in the cssgen contrib module (plus possibly XSS, but it needs upstream to confirm)

www.openwall.com
text/html

[MLIST \[oss-security\] 20120821 Re: CVE Request -- php-geshi / GeSHi \(1.0.8.11\): Remote directory traversal and information disclosure in the cssgen contrib module \(plus possibly XSS, but it needs upstream to confirm\)](#)

[SECURITY] Fedora 18 Update: php-geshi-1.0.8.11-3.fc18

[lists.fedoraproject.org](https://lists.fedoraproject.org/text/html)
text/html

[FEDORA FEDORA-2013-5472](#)

GeSHi - Generic Syntax Highlighter / Code / Commit [r2508]

[Exploit](#)
[Patch](#)
sourceforge.net
text/html

[CONFIRM sourceforge.net/p/geshi/code/2508/](https://sourceforge.net/p/geshi/code/2508/)

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qbnz	Geshi	1.0.8.4	All	All	All
Application	Qbnz	Geshi	1.0.8.5	All	All	All
Application	Qbnz	Geshi	1.0.8.6	All	All	All
Application	Qbnz	Geshi	1.0.8.7	All	All	All
Application	Qbnz	Geshi	1.0.8.8	All	All	All
Application	Qbnz	Geshi	1.0.8.9	All	All	All
Application	Qbnz	Geshi	1.0.8.4	All	All	All
Application	Qbnz	Geshi	1.0.8.5	All	All	All
Application	Qbnz	Geshi	1.0.8.6	All	All	All
Application	Qbnz	Geshi	1.0.8.7	All	All	All
Application	Qbnz	Geshi	1.0.8.8	All	All	All
Application	Qbnz	Geshi	1.0.8.9	All	All	All
Application	Qbnz	Geshi	All	All	All	All

[illegible]

cpe:2.3:a:qbnz:geshi:1.0.8.0:.....
cpe:2.3:a:qbnz:geshi:1.0.8.9:*****:
cpe:2.3:a:qbnz:geshi:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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