



CVE-2011-4357

Published on: 12/10/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:21 AM UTC

CVE-2011-4357

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

Certain versions of [Clearsilver](#) from [Brandon Long](#) contain the following vulnerability:

Format string vulnerability in the p_cgi_error function in python/neo_cgi.c in the Python CGI Kit (neo_cgi) module for Clearsilver 0.10.5 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via format string specifiers that are not properly handled when creating CGI error messages using the cgi_error API function.

CVE-2011-4357 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
[text/html](#)

[XF clearsilver-neocgi-format-string\(71599\)](#)

Debian -- Security Information -- DSA-2355-1
clearsilver

www.debian.org
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-2355](#)

No Description Provided

osvdb.org

[OSVDB 77419](#)

[Inactive Link](#) [Not Archived](#)

About Secunia Research | Flexera

[Vendor Advisory](#)
secunia.com
[Deprecated Link](#)

[SECUNIA 47016](#)

Exploitable Link
text/html

oss-security - CVE Request -- ClearSilver (neo_cgi) -- Format string flaw by processing CGI error messages in Python module

www.openwall.com
text/html

MLIST [oss-security] 20111127 CVE Request -- ClearSilver (neo_cgi) -- Format string flaw by processing CGI error messages in Python module

r919 - clearsilver - ClearSilver templating system - Google Project Hosting

code.google.com
text/html

CONFIRM
code.google.com/p/clearsilver/source/detail?r=919

No Description Provided

tech.groups.yahoo.com

CONFIRM
tech.groups.yahoo.com/group/ClearSilver/message/1422

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	Brandon Long	Clearsilver	0.1	All	All	All
Application	Brandon Long	Clearsilver	0.10.1	All	All	All
Application	Brandon Long	Clearsilver	0.10.2	All	All	All
Application	Brandon Long	Clearsilver	0.10.3	All	All	All
Application	Brandon Long	Clearsilver	0.10.4	All	All	All
Application	Brandon Long	Clearsilver	0.2	All	All	All
Application	Brandon Long	Clearsilver	0.2.1	All	All	All
Application	Brandon Long	Clearsilver	0.3	All	All	All
Application	Brandon Long	Clearsilver	0.4	All	All	All
Application	Brandon Long	Clearsilver	0.5	All	All	All
Application	Brandon Long	Clearsilver	0.6	All	All	All
Application	Brandon Long	Clearsilver	0.7	All	All	All
Application	Brandon Long	Clearsilver	0.7.1	All	All	All
Application	Brandon Long	Clearsilver	0.7.2	All	All	All
Application	Brandon Long	Clearsilver	0.8.0	All	All	All
Application	Brandon Long	Clearsilver	0.8.1	All	All	All
Application	Brandon Long	Clearsilver	0.9.0	All	All	All
Application	Brandon Long	Clearsilver	0.9.1	All	All	All
Application	Brandon Long	Clearsilver	0.9.14	All	All	All
Application	Brandon Long	Clearsilver	0.9.2	All	All	All
Application	Brandon Long	Clearsilver	0.9.3	All	All	All

Application	Brandon Long	Clearsilver	0.9.6	All	All	All
Application	Brandon Long	Clearsilver	0.9.7	All	All	All
Application	Brandon Long	Clearsilver	All	All	All	All
Application	Brandon Long	Clearsilver	0.1	All	All	All
Application	Brandon Long	Clearsilver	0.10.1	All	All	All
Application	Brandon Long	Clearsilver	0.10.2	All	All	All
Application	Brandon Long	Clearsilver	0.10.3	All	All	All
Application	Brandon Long	Clearsilver	0.10.4	All	All	All
Application	Brandon Long	Clearsilver	0.2	All	All	All
Application	Brandon Long	Clearsilver	0.2.1	All	All	All
Application	Brandon Long	Clearsilver	0.3	All	All	All
Application	Brandon Long	Clearsilver	0.4	All	All	All
Application	Brandon Long	Clearsilver	0.5	All	All	All
Application	Brandon Long	Clearsilver	0.6	All	All	All
Application	Brandon Long	Clearsilver	0.7	All	All	All
Application	Brandon Long	Clearsilver	0.7.1	All	All	All
Application	Brandon Long	Clearsilver	0.7.2	All	All	All
Application	Brandon Long	Clearsilver	0.8.0	All	All	All
Application	Brandon Long	Clearsilver	0.8.1	All	All	All
Application	Brandon Long	Clearsilver	0.9.0	All	All	All
Application	Brandon Long	Clearsilver	0.9.1	All	All	All
Application	Brandon Long	Clearsilver	0.9.14	All	All	All
Application	Brandon Long	Clearsilver	0.9.2	All	All	All
Application	Brandon Long	Clearsilver	0.9.3	All	All	All
Application	Brandon Long	Clearsilver	0.9.6	All	All	All
Application	Brandon Long	Clearsilver	0.9.7	All	All	All
cpe:2.3:a:brandon_long:clearsilver:0.1:*:*:*:*:*:						
cpe:2.3:a:brandon_long:clearsilver:0.10.1:*:*:*:*:*:						
cpe:2.3:a:brandon_long:clearsilver:0.10.2:*:*:*:*:*:						
cpe:2.3:a:brandon_long:clearsilver:0.10.3:*:*:*:*:*:						
cpe:2.3:a:brandon_long:clearsilver:0.10.4:*:*:*:*:*:						
cpe:2.3:a:brandon_long:clearsilver:0.2:*:*:*:*:*:						
cpe:2.3:a:brandon_long:clearsilver:0.2.1:*:*:*:*:*:						

cpe:2.3:a:brandon_long:clearsilver:0.3:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.4:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.5:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.6:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.7:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.7.1:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.7.2:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.8.0:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.8.1:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.9.0:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.9.1:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.9.14:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.9.2:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.9.3:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.9.6:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.9.7:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.1:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.10.1:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.10.2:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.10.3:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.10.4:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.2:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.2.1:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.3:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.4:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.5:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.6:*:*:*:*:*:
cpe:2.3:a:brandon_long:clearsilver:0.7:*:*:*:*:*:

cpe:2.3:a:brandon_long:clearsilver:0.7.1:*****:
cpe:2.3:a:brandon_long:clearsilver:0.7.2:*****:
cpe:2.3:a:brandon_long:clearsilver:0.8.0:*****:
cpe:2.3:a:brandon_long:clearsilver:0.8.1:*****:
cpe:2.3:a:brandon_long:clearsilver:0.9.0:*****:
cpe:2.3:a:brandon_long:clearsilver:0.9.1:*****:
cpe:2.3:a:brandon_long:clearsilver:0.9.14:*****:
cpe:2.3:a:brandon_long:clearsilver:0.9.2:*****:
cpe:2.3:a:brandon_long:clearsilver:0.9.3:*****:
cpe:2.3:a:brandon_long:clearsilver:0.9.6:*****:
cpe:2.3:a:brandon_long:clearsilver:0.9.7:*****:

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](#)