

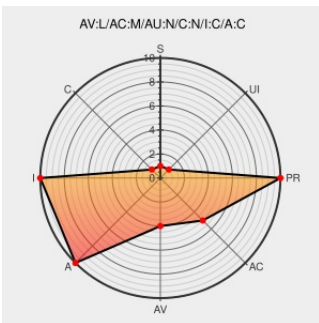


CVE-2011-3616

Published on: 11/04/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:22 AM UTC

CVE-2011-3616

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

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

The `getSkillname` function in the `eve` module in `Conky` 1.8.1 and earlier allows local users to overwrite arbitrary files via a symlink attack on `/tmp/.cesf`.

CVE-2011-3616 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.3 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

oss-security - CVE Request -- Conky 1.8.1 `"/tmp/.cesf"`
Insecure Temporary File Security Issue

www.openwall.com
text/html

MLIST [oss-security] 20111009 CVE Request -- Conky
1.8.1 `"/tmp/.cesf"` Insecure Temporary File Security Issue

Gentoo update for conky - Secunia.com

Vendor Advisory
web.archive.org
text/html

SECUNIA 46353

oss-security - Re: CVE Request -- Conky 1.8.1
`"/tmp/.cesf"` Insecure Temporary File Security Issue

www.openwall.com
text/html

MLIST [oss-security] 20111010 Re: CVE Request --
Conky 1.8.1 `"/tmp/.cesf"` Insecure Temporary File Security
Issue

Gentoo Linux Documentation -- Conky: Privilege
escalation

www.gentoo.org
text/html

GENTOO GLSA-201110-09

#612033 - vulnerability: rewrite arbitrary user file -
Debian Bug report logs

Exploit
bugs.debian.org
text/html

CONFIRM [bugs.debian.org/cgi-bin/bugreport.cgi?](http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=612033)
bug=612033

Conky "/tmp/.cesf" Insecure Temporary File Security
Issue - Advisories - Community

Vendor Advisory

web.archive.org

text/html

 SECUNIA 43225

Bug #607309 "vulnerability: rewrite arbitrary user file" :
Bugs : conky package : Ubuntu

bugs.launchpad.net

text/html

 CONFIRM

bugs.launchpad.net/ubuntu/+source/conky/+bug/607309

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	Conky	Conky	1.1	All	All	All
Application	Conky	Conky	1.2	All	All	All
Application	Conky	Conky	1.3.0	All	All	All
Application	Conky	Conky	1.3.1	All	All	All
Application	Conky	Conky	1.3.2	All	All	All
Application	Conky	Conky	1.3.3	All	All	All
Application	Conky	Conky	1.3.4	All	All	All
Application	Conky	Conky	1.3.5	All	All	All
Application	Conky	Conky	1.4.0	All	All	All
Application	Conky	Conky	1.4.1	All	All	All
Application	Conky	Conky	1.4.2	All	All	All
Application	Conky	Conky	1.4.3	All	All	All
Application	Conky	Conky	1.4.4	All	All	All
Application	Conky	Conky	1.4.5	All	All	All
Application	Conky	Conky	1.4.6	All	All	All
Application	Conky	Conky	1.4.7	All	All	All
Application	Conky	Conky	1.4.8	All	All	All
Application	Conky	Conky	1.4.9	All	All	All
Application	Conky	Conky	1.5.0	All	All	All
Application	Conky	Conky	1.5.1	All	All	All
Application	Conky	Conky	1.6.0	All	All	All
Application	Conky	Conky	1.6.1	All	All	All
Application	Conky	Conky	1.7.0	All	All	All
Application	Conkv	Conkv	1.7.1	All	All	All

cpe:2.3:a:conky:conky:1.3.1:*****:*
cpe:2.3:a:conky:conky:1.3.2:*****:*
cpe:2.3:a:conky:conky:1.3.3:*****:*
cpe:2.3:a:conky:conky:1.3.4:*****:*
cpe:2.3:a:conky:conky:1.3.5:*****:*
cpe:2.3:a:conky:conky:1.4.0:*****:*
cpe:2.3:a:conky:conky:1.4.1:*****:*
cpe:2.3:a:conky:conky:1.4.2:*****:*
cpe:2.3:a:conky:conky:1.4.3:*****:*
cpe:2.3:a:conky:conky:1.4.4:*****:*
cpe:2.3:a:conky:conky:1.4.5:*****:*
cpe:2.3:a:conky:conky:1.4.6:*****:*
cpe:2.3:a:conky:conky:1.4.7:*****:*
cpe:2.3:a:conky:conky:1.4.8:*****:*
cpe:2.3:a:conky:conky:1.4.9:*****:*
cpe:2.3:a:conky:conky:1.5.0:*****:*
cpe:2.3:a:conky:conky:1.5.1:*****:*
cpe:2.3:a:conky:conky:1.6.0:*****:*
cpe:2.3:a:conky:conky:1.6.1:*****:*
cpe:2.3:a:conky:conky:1.7.0:*****:*
cpe:2.3:a:conky:conky:1.7.1:*****:*
cpe:2.3:a:conky:conky:1.7.1.1:*****:*
cpe:2.3:a:conky:conky:1.7.2:*****:*
cpe:2.3:a:conky:conky:1.8.0:*****:*
cpe:2.3:a:conky:conky:1.1:*****:*
cpe:2.3:a:conky:conky:1.2:*****:*
cpe:2.3:a:conky:conky:1.3.0:*****:*
cpe:2.3:a:conky:conky:1.3.1:*****:*
cpe:2.3:a:conky:conky:1.3.2:*****:*

cpe:2.3:a:conky:conky:1.3.2:****:*:*
cpe:2.3:a:conky:conky:1.3.3:****:*:*
cpe:2.3:a:conky:conky:1.3.4:****:*:*
cpe:2.3:a:conky:conky:1.3.5:****:*:*
cpe:2.3:a:conky:conky:1.4.0:****:*:*
cpe:2.3:a:conky:conky:1.4.1:****:*:*
cpe:2.3:a:conky:conky:1.4.2:****:*:*
cpe:2.3:a:conky:conky:1.4.3:****:*:*
cpe:2.3:a:conky:conky:1.4.4:****:*:*
cpe:2.3:a:conky:conky:1.4.5:****:*:*
cpe:2.3:a:conky:conky:1.4.6:****:*:*
cpe:2.3:a:conky:conky:1.4.7:****:*:*
cpe:2.3:a:conky:conky:1.4.8:****:*:*
cpe:2.3:a:conky:conky:1.4.9:****:*:*
cpe:2.3:a:conky:conky:1.5.0:****:*:*
cpe:2.3:a:conky:conky:1.5.1:****:*:*
cpe:2.3:a:conky:conky:1.6.0:****:*:*
cpe:2.3:a:conky:conky:1.6.1:****:*:*
cpe:2.3:a:conky:conky:1.7.0:****:*:*
cpe:2.3:a:conky:conky:1.7.1:****:*:*
cpe:2.3:a:conky:conky:1.7.1.1:****:*:*
cpe:2.3:a:conky:conky:1.7.2:****:*:*
cpe:2.3:a:conky:conky:1.8.0:****:*:*
cpe:2.3:a:conky:conky:****:*:*

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#)