



# CVE-2012-0813

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2012-0813
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-06-29 19:55:02 UTC
<b>Updated</b>	2026-04-29 01:13:23 UTC
<b>Description</b>	Wicd before 1.7.1 saves sensitive information in log files in /var/log/wicd, which allows context-dependent attackers to obtain sensitive information from the process memory.

## Risk And Classification

**Primary CVSS:** v2.0 2.1 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:N/A:N

**Problem Types:** CWE-255 | n/a

## CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:L/AC:L/Au:N/C:P/I:N/A:N

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	David Paleino	Wicd	1.2.7	All	All	All

Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.3.1	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.4.0	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.4.1	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.4.2	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.5.0	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.5.1	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.5.2	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.5.3	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.5.4	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.5.5	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.5.6	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.5.7	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.5.8	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.5.9	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.6.0	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.6.2	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.7.0	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.7.1	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	1.7.2	All	All	All
Application	<a href="#">David Paleino</a>	<a href="#">Wicd</a>	All	beta3	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

### References

Reference	Source
Gentoo Linux Documentation -- Wicd: Multiple vulnerabilities	<a href="#">af854a3a-2127-422b-91ae-364d...</a>
oss-security - Re: CVE request: wicd writes sensitive information in log files (password, passphrase...)	<a href="#">af854a3a-2127-422b-91ae-364d...</a>
#652417 - wicd writes sensitive information in log files (password, passphrase...) - Debian Bug report logs	<a href="#">af854a3a-2127-422b-91ae-364d...</a>
oss-security - CVE request: wicd writes sensitive information in log files (password, passphrase...)	<a href="#">af854a3a-2127-422b-91ae-364d...</a>
Wicd 'wicd/configmanager.py' Local Information Disclosure Vulnerability	<a href="#">af854a3a-2127-422b-91ae-364d...</a>
~wicd-devel/wicd/experimental : revision 682	<a href="#">af854a3a-2127-422b-91ae-364d...</a>
1.7.1 released : wicd	<a href="#">af854a3a-2127-422b-91ae-364d...</a>
About Secunia Research   Flexera	<a href="#">af854a3a-2127-422b-91ae-364d...</a>
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)