



# CVE-2008-0882

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2008-0882
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-02-21 19:44:00 UTC
<b>Updated</b>	2017-09-29 01:30:00 UTC
<b>Description</b>	Double free vulnerability in the process_browse_data function in CUPS 1.3.5 allows remote attackers to cause a denial of s

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Cups</a>	<a href="#">Cups</a>	1.3.5	All	All	All
Application	<a href="#">Cups</a>	<a href="#">Cups</a>	1.3.5	All	All	All

## References

Reference	Source	Lin
Support / Security / Advisories // MDVSA-2008:050   Mandriva	MANDRIVA	<a href="#">ww</a>
Support / Security / Advisories // MDVSA-2008:051   Mandriva	MANDRIVA	<a href="#">ww</a>
About Security Update 2008-002	CONFIRM	<a href="#">doc</a>
SUSE update for cups - Advisories - Secunia	SECUNIA	<a href="#">sec</a>
Ubuntu update for cups - Advisories - Secunia	SECUNIA	<a href="#">sec</a>
Red Hat update for cups - Advisories - Secunia	SECUNIA	<a href="#">sec</a>
Gentoo update for cups - Advisories - Secunia	SECUNIA	<a href="#">sec</a>
STR #2656: cupsd dies due to double freeing of a remote printer - CUPS.org	CONFIRM	<a href="#">ww</a>
[security-announce] SUSE Security Announcement: cups (SUSE-SA:2008:012)	SUSE	<a href="#">list:</a>
Debian -- Security Information -- DSA-1530-1 cupsys	DEBIAN	<a href="#">ww</a>
CUPS "process_browse_data()" Double Free Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="#">sec</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">ww</a>

Repository / Oval Repository	OVAL	<a href="#">ova</a>
Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="#">sec</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">ww</a>
Mandriva update for cups - Advisories - Secunia	SECUNIA	<a href="#">sec</a>
Debian update for cupsys - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="#">sec</a>
[SECURITY] Fedora 7 Update: cups-1.2.12-9.fc7	FEDORA	<a href="#">ww</a>
CUPS Double Free Bug in process_browse_data() May Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="#">ww</a>
CUPS: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO	<a href="#">sec</a>
CUPS 'process_browse_data()' Remote Double Free Denial of Service Vulnerability	BID	<a href="#">ww</a>
[SECURITY] Fedora 8 Update: cups-1.3.6-2.fc8	FEDORA	<a href="#">ww</a>
Fedora update for cups - Advisories - Secunia	SECUNIA	<a href="#">sec</a>
USN-598-1: CUPS vulnerabilities   Ubuntu	UBUNTU	<a href="#">ww</a>
rhn.redhat.com   Red Hat Support	REDHAT	<a href="#">ww</a>
Bug 433758 – CVE-2008-0882 cups: double free vulnerability in process_browse_data()	CONFIRM	<a href="#">bu</a>
APPLE-SA-2008-03-18 Security Update 2008-002	APPLE	<a href="#">list</a>
CVE Program record	CVE.ORG	<a href="#">ww</a>
NVD vulnerability detail	NVD	<a href="#">nvd</a>

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](#).

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