



CVE-2014-4337

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-4337
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-22 21:55:00 UTC
Updated	2018-01-08 15:22:00 UTC
Description	The process_browse_data function in utils/cups-browsed.c in cups-browsed in cups-filters before 1.0.53 allows remote attar

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Cups-filters	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - Re: cups-browsed remote exploit	MLIST	openwall.com	Mailing List
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party Advisory
cups-filters CVE-2014-4337 Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB Er
/openprinting/cups-filters : revision 7194	CONFIRM	bzd.linuxfoundation.org	Patch
Security Advisory SA62044 - Red Hat update for cups-filters - Secunia	SECUNIA	secunia.com	Permissions Required
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#)