



CVE-2012-4505

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

Summary

CVE	CVE-2012-4505
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-11 13:00:00 UTC
Updated	2023-11-07 02:11:00 UTC
Description	Heap-based buffer overflow in the px_pac_reload function in lib/pac.c in libproxy 0.2.x and 0.3.x allows remote servers to h

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libproxy Project	Libproxy	0.2.3	All	All	All
Application	Libproxy Project	Libproxy	0.3.0	All	All	All
Application	Libproxy Project	Libproxy	0.3.1	All	All	All
Application	Libproxy Project	Libproxy	0.2.3	All	All	All
Application	Libproxy Project	Libproxy	0.3.0	All	All	All
Application	Libproxy Project	Libproxy	0.3.1	All	All	All

References

Reference	Source
USN-1629-1: libproxy vulnerabilities Ubuntu	UBUNTU
Debian -- Security Information -- DSA-2571-1 libproxy	DEBIAN
Security Advisory SA51048 - SUSE update for libproxy - Secunia	SECUNIA
Security Advisory SA51308 - Red Hat update for libproxy - Secunia	SECUNIA
oss-security - Re: libproxy PAC downloading buffer overflows	MLIST
libproxy CVE-2012-4505 Heap-Based Buffer Overflow Vulnerability	BID
Red Hat Customer Portal	REDHAT
oss-security - Re: libproxy PAC downloading buffer overflows	MLIST

Google Groups	
openSUSE-SU-2012:1375-1: moderate: update for libproxy, libproxy-plugins	SUSE
Security Advisory SA51180 - Debian update for libproxy - Secunia	SECUNIA
oss-security - libproxy PAC downloading buffer overflows	MLIST
864612 – (CVE-2012-4505) CVE-2012-4505 libproxy: PAC handling insufficient content length check leading to buffer overflow	CONFIRM
Google Groups	CONFIRM
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](#).

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