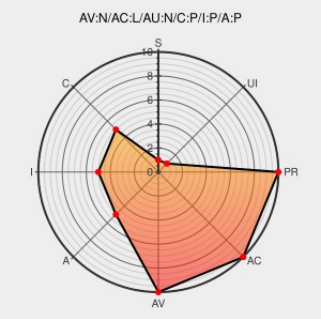
CVE-2015-1031

Published on: 02/10/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:10 PM UTC

CVE-2015-1031

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Privoxy from Privoxy contain the following vulnerability:

Multiple use-after-free vulnerabilities in Privoxy before 3.0.22 allow remote attackers to have unspecified impact via vectors related to (1) the unmap function in list.c or (2) "two additional unconfirmed use-after-free complaints made by Coverity scan." NOTE: some of these details are obtained from third party information.

CVE-2015-1031 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Advisory SA62123 - Privoxy Multiple Vulnerabilities - Secunia	web.archive.org, text/html	SECUNIA 62123
	Patch, Vendor Advisory, www.privoxy.org, text/plain	CONFIRM www.privoxy.org/announce.txt
oss-security - Re: CVE Request for Privoxy Version: 3.0.22	www.openwall.com, text/html	MLIST [oss-security] 20150110 Re: CVE Request for Privoxy Version: 3.0.22
Debian -- Security Information -- DSA-3133-1 privoxy	Vendor Advisory, www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3133

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	Privoxy	Privoxy	All	All	All	All

cpe:2.3:a:privoxy:privoxy:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→