

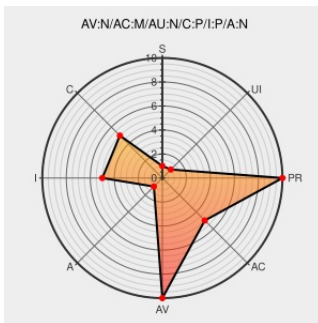


CVE-2013-2503

Published on: 03/11/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:42 PM UTC

CVE-2013-2503

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Privoxy](#) from [Privoxy](#) contain the following vulnerability:

Privoxy before 3.0.21 does not properly handle Proxy-Authenticate and Proxy-Authorization headers in the client-server data stream, which makes it easier for remote HTTP servers to spoof the intended proxy service via a 407 (aka Proxy Authentication Required) HTTP status code.

CVE-2013-2503 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
CVS Info for project ijbswa	ijbswa.cvs.sourceforge.net text/html	CONFIRM ijbswa.cvs.sourceforge.net/viewvc/ijbswa/current/ChangeLog?revision=1.188&view=markup
Privoxy Proxy Authentication Credential Exposure – CVE-2013-2503 Catch ²² (in)security / ChrisJohnRiley	Exploit blog.c22.cc text/html	MISC blog.c22.cc/2013/03/11/privoxy-proxy-authentication-credential-exposure-cve-2013-2503/
openSUSE-SU-2013:0564-1: moderate: privoxy: update to 3.0.21 to fix secu	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0564

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

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	2.9.0	pre-alpha	All	All
Application	Privoxy	Privoxy	2.9.1	pre-alpha	All	All
Application	Privoxy	Privoxy	2.9.11	alpha	All	All
Application	Privoxy	Privoxy	2.9.11	beta	All	All
Application	Privoxy	Privoxy	2.9.11	pre-alpha	All	All
Application	Privoxy	Privoxy	2.9.12	beta	All	All
Application	Privoxy	Privoxy	2.9.13	beta	All	All
Application	Privoxy	Privoxy	2.9.14	beta	All	All
Application	Privoxy	Privoxy	2.9.16	All	All	All
Application	Privoxy	Privoxy	2.9.18	All	All	All
Application	Privoxy	Privoxy	2.9.2	pre-alpha	All	All
Application	Privoxy	Privoxy	2.9.3	pre-alpha	All	All
Application	Privoxy	Privoxy	3.0	All	All	All
Application	Privoxy	Privoxy	3.0.10	All	All	All
Application	Privoxy	Privoxy	3.0.11	All	All	All
Application	Privoxy	Privoxy	3.0.12	All	All	All
Application	Privoxy	Privoxy	3.0.13	beta	All	All
Application	Privoxy	Privoxy	3.0.14	beta	All	All
Application	Privoxy	Privoxy	3.0.15	beta	All	All
Application	Privoxy	Privoxy	3.0.16	All	All	All
Application	Privoxy	Privoxy	3.0.17	All	All	All
Application	Privoxy	Privoxy	3.0.18	All	All	All
Application	Privoxy	Privoxy	3.0.19	All	All	All
Application	Privoxy	Privoxy	3.0.2	All	All	All
Application	Privoxy	Privoxy	3.0.3	All	All	All
Application	Privoxy	Privoxy	3.0.5	beta	All	All
Application	Privoxy	Privoxy	3.0.6	All	All	All
Application	Privoxy	Privoxy	3.0.7	beta	All	All
Application	Privoxy	Privoxy	3.0.8	All	All	All
Application	Privoxy	Privoxy	3.0.9	beta	All	All

cpe:2.3:a:privoxy:privoxy:2.9.11:beta:*****:
cpe:2.3:a:privoxy:privoxy:2.9.11:pre-alpha:*****:
cpe:2.3:a:privoxy:privoxy:2.9.12:beta:*****:
cpe:2.3:a:privoxy:privoxy:2.9.13:beta:*****:
cpe:2.3:a:privoxy:privoxy:2.9.14:beta:*****:
cpe:2.3:a:privoxy:privoxy:2.9.16:*****:
cpe:2.3:a:privoxy:privoxy:2.9.18:*****:
cpe:2.3:a:privoxy:privoxy:2.9.2:pre-alpha:*****:
cpe:2.3:a:privoxy:privoxy:2.9.3:pre-alpha:*****:
cpe:2.3:a:privoxy:privoxy:3.0:*****:
cpe:2.3:a:privoxy:privoxy:3.0.10:*****:
cpe:2.3:a:privoxy:privoxy:3.0.11:*****:
cpe:2.3:a:privoxy:privoxy:3.0.12:*****:
cpe:2.3:a:privoxy:privoxy:3.0.13:beta:*****:
cpe:2.3:a:privoxy:privoxy:3.0.14:beta:*****:
cpe:2.3:a:privoxy:privoxy:3.0.15:beta:*****:
cpe:2.3:a:privoxy:privoxy:3.0.16:*****:
cpe:2.3:a:privoxy:privoxy:3.0.17:*****:
cpe:2.3:a:privoxy:privoxy:3.0.18:*****:
cpe:2.3:a:privoxy:privoxy:3.0.19:*****:
cpe:2.3:a:privoxy:privoxy:3.0.2:*****:
cpe:2.3:a:privoxy:privoxy:3.0.3:*****:
cpe:2.3:a:privoxy:privoxy:3.0.5:beta:*****:
cpe:2.3:a:privoxy:privoxy:3.0.6:*****:
cpe:2.3:a:privoxy:privoxy:3.0.7:beta:*****:
cpe:2.3:a:privoxy:privoxy:3.0.8:*****:
cpe:2.3:a:privoxy:privoxy:3.0.9:beta:*****:
cpe:2.3:a:privoxy:privoxy:2.9.0:pre-alpha:*****:
cpe:2.3:a:privoxy:privoxy:2.9.1:pre-alpha:*****:

cpe:2.3:a:privoxy:privoxy:2.9.11:alpha:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:2.9.11:beta:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:2.9.11:pre-alpha:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:2.9.12:beta:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:2.9.13:beta:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:2.9.14:beta:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:2.9.16:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:2.9.18:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:2.9.2:pre-alpha:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:2.9.3:pre-alpha:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.10:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.11:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.12:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.13:beta:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.14:beta:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.15:beta:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.16:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.17:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.18:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.19:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.2:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.3:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.5:beta:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.6:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.7:beta:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.8:~::~~::~~::~~::~~::
cpe:2.3:a:privoxy:privoxy:3.0.9:beta:~::~~::~~::~~::~~::

cpe:2.3:a:privoxy:privoxy:*:beta:*:*:*:*.*

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023  |

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](#)