



CVE-2021-20209

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

Summary

CVE	CVE-2021-20209
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-25 20:15:00 UTC
Updated	2023-11-07 03:29:00 UTC
Description	A memory leak vulnerability was found in Privoxy before 3.0.29 in the show-status CGI handler when no action files are cor

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Privoxy	Privoxy	All	All	All	All

References

Reference	S
www.privoxy.org Git - privoxy.git/commit	M
1928726 – (CVE-2021-20209) CVE-2021-20209 privoxy: memory leak in the show-status CGI handler when no action files are configured	M
What's New in this Release	M
www.privoxy.org Git - privoxy.git/commit	
Privoxy: Multiple vulnerabilities (GLSA 202107-16) — Gentoo security	C
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180317](#) Debian Security Update for privoxy (CVE-2021-20209)

[198306](#) Ubuntu Security Notification for Privoxy Vulnerabilities (USN-4886-1)

© [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](#)