



CVE-2020-4042

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-4042
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-10 20:15:00 UTC
Updated	2020-07-15 17:30:00 UTC
Description	Bareos before version 19.2.8 and earlier allows a malicious client to communicate with the director without knowledge of the

Risk And Classification

Problem Types: CWE-294

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bareos	Bareos	19.2.8	pre	All	All
Application	Bareos	Bareos	19.2.8	pre	All	All
Application	Bareos	Bareos	All	All	All	All

References

Reference	Source	Link
Authentication bypass in director when allowing client and director initiated connections · Advisory · bareos/bareos · GitHub	CONFIRM	git
0001250: Authentication bypass in Director when allowing client and director initiated connections - Bareos Bug Tracker	MISC	bu
CVE Program record	CVE.ORG	vv
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501528](#) Alpine Linux Security Update for bareos

[504585](#) Alpine Linux Security Update for bareos

© [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](#).

Free CVE JSON API [cve.report/api](#)

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