



CVE-2023-43320

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

Summary

CVE	CVE-2023-43320
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-27 23:15:00 UTC
Updated	2024-02-02 17:15:00 UTC
Description	An issue in Proxmox Server Solutions GmbH Proxmox VE v.5.4 thru v.8.0, Proxmox Backup Server v.1.1 thru v.3.0, and Pr

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Proxmox	Backup Server	All	All	All	All
Application	Proxmox	Proxmox Mail Gateway	All	All	All	All
Application	Proxmox	Virtual Environment	All	All	All	All

References

Reference	Source	Link	Tags
Proxmox VE 7.4-1 TOTP Brute Force ≈ Packet Storm		packetstormsecurity.com	
4584 – restrict user after multiple failed TOTP second factor auth tries in a row	MISC	bugzilla.proxmox.com	
4579 – Improve resiliency against TOTP brute force if account credentials already leaked	MISC	bugzilla.proxmox.com	
tfa: add data for rate limiting and blocking · proxmox/proxmox-rs@50b793d · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

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](#).

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

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