



CVE-2026-29200

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

Summary

CVE	CVE-2026-29200
State	PUBLISHED
Assigner	hackerone
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 07:16:00 UTC
Updated	2026-05-06 19:05:56 UTC
Description	A critical IDOR vulnerability has been discovered in Comet Backup affecting all versions from 20.11.0 to 26.1.1 and 26.2.1.

Risk And Classification

Primary CVSS: v4.0 9.9 CRITICAL from support@hackerone.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-639 | CWE-639 CWE-639 Insecure Direct Object Reference (IDOR)

Version	Source	Type	Score	Severity	Vector
4.0	support@hackerone.com	Secondary	9.9	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/S
4.0	CNA	DECLARED	9.9	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WebPros	Comet Backup	affected 20.11.0 26.1.2 semver	Not specified
CNA	WebPros	Comet Backup	affected 26.2.0 26.2.2 semver	Not specified

References

Reference	Source	Link
support.cometbackup.com/hc/en-us/articles/40090945484823--CVE-2026-29200-%D0%A1ritica...	support@hackerone.com	support.cometbackup.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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