



CVE-2020-8289

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

Summary

CVE	CVE-2020-8289
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-27 02:15:00 UTC
Updated	2020-12-31 19:04:00 UTC
Description	Backblaze for Windows before 7.0.1.433 and Backblaze for macOS before 7.0.1.434 suffer from improper certificate validation

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Full Disclosure: Re: CVE-2020-8150 – Remote Code Execution as SYSTEM/root via Backblaze	FULLDISC	seclists.org
CVE-2020-8289 – Remote Code Execution as SYSTEM/root via Backblaze (Windows PoC) - YouTube	MISC	youtu.be
HackerOne	MISC	hackerone.com
CVE-2020-8289/README.md at master · geffner/CVE-2020-8289 · GitHub	MISC	github.com
Full Disclosure: Re: [FD] CVE-2020-8150 – Remote Code Execution as SYSTEM/root via Backblaze	FULLDISC	seclists.org
Backblaze Cloud Backup Release 7.0.1	MISC	www.backblaze.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](#)