



CVE-2020-10138

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

Summary

CVE	CVE-2020-10138
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-21 14:15:00 UTC
Updated	2021-12-20 22:24:00 UTC
Description	Acronis Cyber Backup 12.5 and Cyber Protect 15 include an OpenSSL component that specifies an OPENSSLDIR variable

Risk And Classification

Problem Types: CWE-665

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Acronis	Cyber Backup	All	All	All	All
Application	Acronis	Cyber Backup	All	All	All	All
Application	Acronis	Cyber Protect	All	All	All	All
Application	Acronis	Cyber Protect	All	All	All	All

References

Reference	Source	Link	Tags
VU#114757 - Acronis backup software contains multiple privilege escalation vulnerabilities	MISC	www.kb.cert.org	Third Party Advis
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

Vendor Comments And Credit

Discovery Credit

LEGACY: Will Dormann

Legacy QID Mappings

[376220](#) Acronis Cyber Protect Arbitrary Code Execution Vulnerability

© [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](#)