



Published on: Not Yet Published

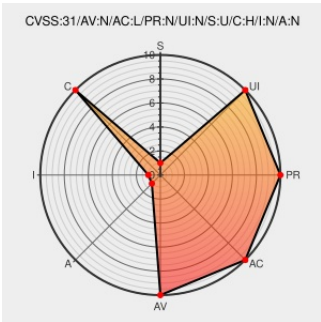
Last Modified on: 05/26/2023 04:56:00 PM UTC

CVE-2022-45450

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Agent](#) from [Acronis](#) contain the following vulnerability:

Sensitive information disclosure and manipulation due to improper authorization. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 28610, Acronis Cyber Protect 15 (Linux, macOS, Windows) before build 30984.

CVE-2022-45450 has been assigned by  security@acronis.com to track the vulnerability - currently rated as  severity.

Affected Vendor/Software: **Acronis - Acronis Agent** version < **28610**

Affected Vendor/Software: **Acronis - Acronis Cyber Protect 15** version < 30984

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
Acronis Advisory Database - Acronis	security-advisory.acronis.com text/html	A MISC security-advisory.acronis.com/advisories/SEC-2410

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Acronis	Agent	All	All	All	All
Application	Acronis	Cyber Protect	All	All	All	All
Application	Acronis	Cyber Protect	15	-	All	All
Application	Acronis	Cyber Protect	15	update1	All	All
Application	Acronis	Cyber Protect	15	update2	All	All
Application	Acronis	Cyber Protect	15	update3	All	All
Application	Acronis	Cyber Protect	15	update4	All	All
Operating System	Apple	Macos	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
cpe:2.3:a:acronis:agent:~::~::~:						
cpe:2.3:a:acronis:cyber_protect:~::~::~:						
cpe:2.3:a:acronis:cyber_protect:15:-::~::~:						
cpe:2.3:a:acronis:cyber_protect:15:update1:~::~::~:						
cpe:2.3:a:acronis:cyber_protect:15:update2:~::~::~:						
cpe:2.3:a:acronis:cyber_protect:15:update3:~::~::~:						
cpe:2.3:a:acronis:cyber_protect:15:update4:~::~::~:						
cpe:2.3:o:apple:macos:-::~::~:						
cpe:2.3:o:linux:linux_kernel:-::~::~:						
cpe:2.3:o:microsoft:windows:-::~::~:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVereport	CVE-2022-45450 : Sensitive information disclosure and manipulation due to improper authorization. The following pro... twitter.com/i/web/status/1...	2023-05-18 10:05:36

© [CVE.report](#) 2023   |

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](#)