



# CVE-2026-41220

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-41220  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | Acronis   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-04-29 15:16:05 UTC   |
| <b>Updated</b>         | 2026-04-30 15:48:26 UTC   |
| <b>Description</b>     | Local privilege escalation due to improper input validation. The following products are affected: Acronis DeviceLock DLP (V |

## Risk And Classification

**Primary CVSS:** v3.0 7.8 HIGH from security@acronis.com

**CVSS:**3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**Problem Types:** CWE-787 | CWE-787 CWE-787

| Version | Source               | Type      | Score | Severity | Vector                                       |
|---------|----------------------|-----------|-------|----------|--|
| 3.0     | security@acronis.com | Secondary | 7.8   | HIGH     | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| 3.0     | CNA                  | CVSS      | 7.8   | HIGH     | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |

## CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

### Vendor Declared Affected Products

| Source | Vendor  | Product                           | Version                               | Platforms |
|--------|---------|-----------------------------------|---------------------------------------|-----------|
| CNA    | Acronis | Acronis DeviceLock DLP            | affected unspecified 9.0.93212 semver | Windows   |
| CNA    | Acronis | Acronis Cyber Protect Cloud Agent | affected unspecified 42183 semver     | Windows   |

### References

| Reference  | Source               | Link  | Tags                |
|--|----------------------|---|---------------------|
| security-advisory.acronis.com/advisories/SEC-10296 | security@acronis.com | <a href="https://security-advisory.acronis.com">security-advisory.acronis.com</a> |                     |
| CVE Program record                                 | CVE.ORG              | <a href="https://www.cve.org">www.cve.org</a>                                     | canonical           |
| NVD vulnerability detail                           | NVD                  | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                                   | canonical, analysis |

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Kolja Grassmann (Neodyme AG) (<mailto:contact@neodyme.io>) (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

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

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)