CVE-2026-41220

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

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

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	security-advisory.acronis.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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.