Velociraptor EVTX Parser — Process Crash via Crafted .evtx File

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

Summary

CVE	CVE-2026-7572
State	PUBLISHED
Assigner	rapid7
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 03:15:58 UTC
Updated	2026-05-06 03:15:58 UTC
Description	An off-by-one error (CWE-193) in the ConsumeUnit16Array and ConsumeUnit64Array functions in Velocidex Velociraptor b

Risk And Classification

Primary CVSS: v3.1 4.4 MEDIUM from cve@rapid7.com

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L

Problem Types: CWE-193 | CWE-193 CWE-193: Off-by-one Error

Version	Source	Type	Score	Severity	Vector
3.1	cve@rapid7.com	Secondary	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L
3.1	CNA	CVSS	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
None

User Interaction
Required

Scope
Unchanged

Confidentiality
None

Integrity
Low

Availability

Low

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Velocidex	Velociraptor	affected 0.76.5 semver	Windows, Linux

References

Reference	Source	Link	Tags
docs.velociraptor.app/announcements/advisories/cve-2026-7572	cve@rapid7.com	docs.velociraptor.app	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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