CVE-2026-7572 Velociraptor EVTX Parser — Process Crash Via Crafted .Evtx File

Published on 2026-05-04

▶ CVSS · MEDIUM · 5.1 /10

An off-by-one error (CWE-193) in the ConsumeUnit16Array and ConsumeUnit64Array functions in Velocidex Velociraptor up to version 0.76.1 on Windows and Linux allows a local attacker to cause a Denial of Service (DoS) via a process crash by providing a specially crafted .evtx file to the parse_evtx VQL plugin.

Required configuration for exposure:

This vulnerability only affects users who use artifacts that parse the EVTX files. Those artifacts will cause the client to crash, which will be reported to the server.

An effective workaround is to switch to artifacts that collect the raw evtx files (e.g. the Windows.Triage.Targets artifact) and parse these offline on the server.

Problem:

CWE-193: Off-by-one Error CWE-193

Impact:

CAPEC-617: Reachable Assertion CAPEC-617

Product Status:

Product	Affected
Rapid7 Velociraptor *on* Linux source repo Default status is unaffected	before 0.76.5

Credits:

We thank Javier Perez for identifying and reporting this issue responsibly

References

docs.velociraptor.app/announcements/advisories/cve-2026-7572/

Recommendation

This vulnerability will result in a client crash when parsing a malicious evtx file (e.g. using the `Windows.EventLogs.EvtxHunter` artifact). If this occurs users can switch to collecting the raw EVTX files using bulk collection artifacts like `Windows.Triage.Targets` or `Windows.Search.FileFinder` and parse the files offline.

Alternatively, you can upgrade your client to the latest version:

- For 0.76 releases, upgrade to v0.76.5