CVE-2026-7573 GetUserRoles API Endpoint Allows Any Authenticated User To Enumerate ACL Policies Across All Organizations

Published on 2026-05-04

▶ CVSS · MEDIUM · 5.1 /10

An authorization bypass (CWE-639) in the GetUserRoles gRPC API endpoint in Velocidex Velociraptor up to version 0.76.3 allows any authenticated low-privilege user to retrieve the complete ACL policy (roles and permissions) for any user across all organizations by supplying targeted Name and Org parameters via a network request.

Problem:

CWE-639: Authorization Bypass Through User-Controlled Key CWE-639

Impact:

CAPEC-37: Retrieve Embedded Sensitive Data CAPEC-37

Product Status:

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

Credits:

We thank Michael Dickenson for identifying and reporting this issue responsibly

References

docs.velociraptor.app/announcements/advisories/cve-2026-7573/

Recommendation

Exploiting this vulnerability requires the attacker to already know the org id and user name of the target users. The additional information obtained is restricted to the target user's roles and permissions within the target org. Attackers can not directly use this information, other than to concentrate on compromising high privilege accounts.

We recommend securing all high privilege Velociraptor user accounts using 2 factor, and SSO to prevent further attacks on those accounts.

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

- For 0.76 releases, upgrade to v0.76.5