CRITICAL

CV_2026_07_9: Improper Authorization Validation

AdvisoryID: CV_2026_07_9

Severity: Critical

Issued: 2026-08-11

Updated: 2026-08-11

CVE.Org link: CVE-2026-13738

Summary

CommServe contained an authorization bypass vulnerability affecting a limited set of command execution operations.

Software customer upgrade to resolved maintenance release.

CVSS score: 9.2

Commvault Software

To view version support lifecyle, see Commvault software releases, release types, and release tracks.

Versions not listed are out of support or unaffected.

Product	Platforms	Affected Versions	Resolved Version	Status
Commvault	Linux, Windows	11.46.0 - 11.46.9	11.46.10 and above	Resolved
Commvault	Linux, Windows	11.44.0 - 11.44.10	11.44.11 and above	Resolved
Commvault	Linux, Windows	11.40.0 - 11.40.62	11.40.63 and above	Resolved
Commvault	Linux, Windows	11.36.0 - 11.36.113	11.36.114 and above	Resolved

Resolution

Software customers upgrade to resolved maintenance release. Update all Commvault installations, including Commserve, Webserver, Command Center, Media Agents, Clients and HyperScale X.

FAQ

How to verify if updates are installed?

To verify updates, log into Command Center and navigate to **Manage > Servers** (or **Manage -> Infrastructure -> Servers**). Filter servers by relevant role, for example, Web Server role. View updates in the Server listing page and confirm all servers are updated with the resolved maintenance release or a higher version.