Security Vulnerability - Lasernet Keep and Autoform DM

2026-06-11 - Angela Simms - Comments (0) - General

The Lasernet Group has identified a cybersecurity vulnerability (R250326) that affects customers using certain versions of Lasernet Keep and Autoform DM.

Cloud Customers - No Action Required

No action is required from cloud customers. This security vulnerability has already been resolved, and the required hotfix has been deployed across all cloud environments.

Vulnerability Details

The role service allows privilege escalation for db-local user accounts.

Affected Versions

The following table shows which versions are affected and the appropriate action to take:

Application and version	Vulnerable	Action to take
Autoform DM 10.0.0 or earlier	No	None
Autoform DM 10.0.0 to 10.5.4	Yes	Upgrade to Autoform DM 10.5.5 or apply the security hotfix.
Autoform DM 10.5.5 or later	No	None
Lasernet Keep 11.0.0	Yes	Upgrade to Keep 11.1.1.
Lasernet Keep 11.1.0 or later	No	None

Available Fixes

If you have installed one of the affected versions, we encourage you to apply the following fixes as soon as possible. For more information and support, contact Lasernet Support.

Lasernet Keep 11.0

Upgrade to Lasernet Keep 11.1.1.

- Lasernet Keep 11.1.1 Release Notes

Autoform DM 10.0.0 to 10.5.4

The Lasernet Group recommends upgrading to Autoform DM 10.5.5. However, if an upgrade is not currently feasible, you can apply the Security Hotfix R250326 on an existing Autoform DM installation and plan to upgrade at the earliest opportunity.

- Autoform DM 10.5.5 Release Notes
- Security Hotfix R250326