Information Disclosure Vulnerability in Autoform DM

2024-02-28 - Sunil Panchal - Comments (0) - Autoform DM News

Autoform DM

An information disclosure vulnerability has been identified in Autoform DM. This vulnerability can result in the exposure of sensitive information to unauthorized and malicious actors, including:

- Details about the environment that Autoform DM is running in.
- The Autoform DM version.
- Aspects of the current Autoform DM configuration.

This exposure is caused by a file that generates information to aid configuration and debugging of a legacy Autoform DM capability. This file's presence is not advertised, and it is not possible to discover the generated information through the Autoform DM web application. However, any malicious actor that is aware of the URL path to the information would be able to access it.

This vulnerability affects Autoform DM 8.0.0 and later.

Resolution — Cloud Deployments

Formpipe has updated all Cloud deployments to remove the vulnerability. Responsive management of Formpipe solutions is a key benefit of being a Formpipe Cloud customer.

No further action is required from the customer.

Resolution — Self-Hosted Deployments

To remove the vulnerability as soon as possible, Formpipe strongly encourages customers to either upgrade Autoform DM or patch their currently installed Autoform DM version. Removing the vulnerability is especially important if Autoform DM can be accessed from outside the customer's internal networks.

Upgrade

For self-hosted deployments, Formpipe advises upgrading to the Autoform DM 10.4.1 maintenance release. This release fixes the vulnerability.

Patch

Vulnerability removal solutions that do not require an upgrade are available for Autoform DM versions 9.0.0 and later. These solutions are suitable if it is not feasible to upgrade Autoform DM. For further information, see Patching. If the customer is running an Autoform DM version earlier than 9.0.0, see Further Assistance for information on how to contact Formpipe Support.

Note

In addition to upgrading or patching Autoform DM, customers should review the Autoform DM Security Hardening guide to ensure that they are following best practices for keeping the product secure, including implementing whitelists (if appropriate).

Patching

A package that provides everything necessary to remove the vulnerability from existing deployments is available. Patch Autoform DM in scenarios where an upgrade is not feasible.

To download the package, click this link: https://prsupportdownloads.blob.core.windows.net/autoformdm/Tools/ha-ear-patcher-1.0.0-dist.zip

The package supports two distinct approaches for removing the vulnerability:

- Through Autoform DM configuration, block access to the URL path to the information.
- Remove the file from Autoform DM.

For information on how to apply either solution, refer to the documentation that is included in the package.

The process has been thoroughly tested and verified. Either of the two approaches will resolve this issue, so customers can apply their preferred solution.

Further Assistance

If any further guidance or assistance is required, contact Formpipe Support via the **Create Ticket** button in the support portal.