

# SCT, CCT, and Metasys Server Patch

## 1 FIX PROVIDED BY PATCH

A vulnerability exists that could be exploited by an attacker to attain unauthorized access to SQL Server Express that SCT, CCT and Metasys software uses. This vulnerability is specific to SQL Express, and does NOT apply to other SQL Server editions. The data in the SQL Server Express databases could be exposed, tampered with or deleted. The provided script will disable an unused SQL login and we recommend you block or secure port 1433 used for remote SQL connections.

This affects all machines where a SCT, CCT or Metasys installer has been used to install SQL Express. Metasys installers which install SQL express include NAE85, LCS85, ADS Lite-A, ADS Lite-E, ADS, ADX, OAS, CCT, SCT/JCT. Refer to flash sheet LIT-2025F17 for a detailed list of affected products and versions, as well as alternative installer downloads that address the issue.

Remote SQL connections are not required by SCT, CCT or Metasys, when the database resides on the same server as the application. Therefore, you are advised to block port 1433, used for SQL server remote connections, unless you have software that integrates remotely with the database, such as OpenBlue Bridge with the Metasys SQL Connector. If remote SQL connections are needed, then create a separate firewall rule which only allows inbound TCP port 1433 traffic from the IP address of the machine that needs this access.

Refer to flash sheet LIT-2025F17 for detailed instructions on blocking port 1433.

Additional enhanced security measures can be found in the Metasys Hardening Guide available at <https://www.johnsoncontrols.com/trust-center/cybersecurity/resources>

## 2 PATCH CONTENTS

The patch is comprised of the following files:

- **GIV-165989-fix-batch.bat** – A batch file which invokes the GIV-165989-fix-ps.ps1 PowerShell script
- **GIV-165989-fix-ps.ps1** – A PowerShell script file which applies the patch to SQL Server.

## 3 Patch Installation

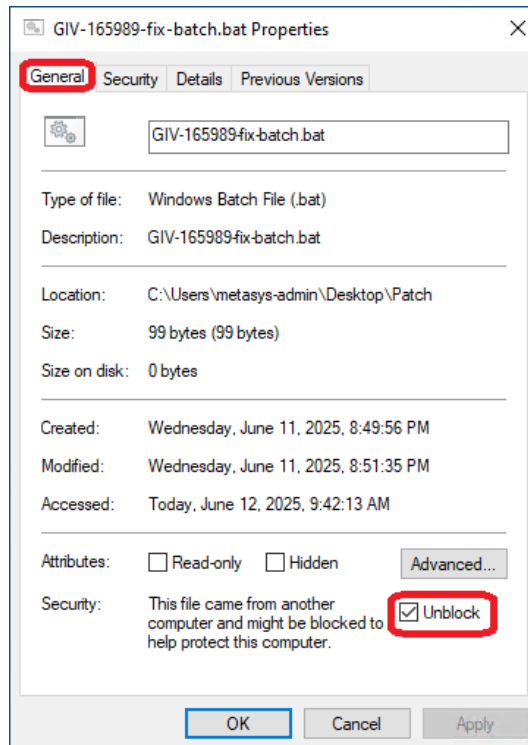
**Prerequisite:** PowerShell must be installed on the machine hosting SCT, CCT, or Metasys Server and the logged in user must have admin rights to the database using Windows Authentication.

To apply the patch:

1. Copy the following files to a folder of your choice under your account on the machine

hosting Metasys and/or SCT:

1. **GIV-165989-fix-batch.bat**
  2. **GIV-165989-fix-ps.ps1**
2. Right click on **GIV-165989-fix-batch.bat** file and click properties. If you see the Unblock checkbox at the bottom, check this box and click OK.



3. Right click on **GIV-165989-fix-batch.bat** file and run it as Administrator or JCI elevated (if running on a JCI machine). This will launch the **GIV-165989-fix-ps.ps1** PowerShell script.

