SSA-472448: Security Bypass Vulnerability in the SQL Client-Server Communication in Siveillance Video

Publication Date: 2024-11-13
Last Update: 2024-11-13
Current Version: V1.0
CVSS v3.1 Base Score: 8.7

SUMMARY

Siveillance Video is affected by a security bypass vulnerability in the Microsoft .NET implementation of SQL Client as described in CVE-2024-0056.

Siemens has released new versions for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Siveillance Video 2022 R1: All versions < V22.1 HotfixRev16 affected by CVE-2024-0056	Update to V22.1 HotfixRev16 or later version https://support.industry.siemens.com/cs/ww/en/view/109810201/
Siveillance Video 2022 R2: All versions < V22.2 HotfixRev16 affected by CVE-2024-0056	Update to V22.2 HotfixRev16 or later version https://support.industry.siemens.com/cs/ww/en/view/109812608/
Siveillance Video 2022 R3: All versions < V22.3 HotfixRev15 affected by CVE-2024-0056	Update to V22.3 HotfixRev15 or later version https://support.industry.siemens.com/cs/ww/en/view/109815353/
Siveillance Video 2023 R1: All versions < V23.1 HotfixRev14 affected by CVE-2024-0056	Update to V23.1 HotfixRev14 or later version https://support.industry.siemens.com/cs/ww/en/view/109820659/
Siveillance Video 2023 R2: All versions < V23.2 HotfixRev13 affected by CVE-2024-0056	Update to V23.2 HotfixRev13 or later version https://support.industry.siemens.com/cs/ww/en/view/109823922/
Siveillance Video 2023 R3: All versions < V23.3 HotfixRev11 affected by CVE-2024-0056	Update to V23.3 HotfixRev11 or later version https://support.industry.siemens.com/cs/ww/en/view/109827783/

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

Siveillance Video (formerly called Siveillance VMS) is a powerful IP video management software designed for deployments ranging from small and simple to large-scale and high-security. The Siveillance Video portfolio consists of four versions, Siveillance Video Core, Core Plus, Advanced, and Pro, addressing the specific needs of small and medium size solutions up to large complex deployments.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2024-0056

Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass Vulnerability

CVSS v3.1 Base Score	8.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N
CWE	CWE-319: Cleartext Transmission of Sensitive Information

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Milestone PSIRT for reporting and coordinated disclosure

ADDITIONAL INFORMATION

For additional information regarding the vulnerability see

- Related Milestone Security Advisory: https://supportcommunity.milestonesys.com/s/article/SQL-Client-possible-Security-Feature-Bypass
- Vulnerability details for Microsoft .NET's System.Data.SqlClient and Microsoft.Data.SqlClient NuGet Packages: https://github.com/dotnet/announcements/issues/292

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2024-11-13): Publication Date

TERMS OF USE

The use of Siemens Security Advisories is subject to the terms and conditions listed on: https://www.siemens.com/productcert/terms-of-use.