SSA-770698: User Information Disclosure Vulnerability in Siveillance Video Client

Publication Date:	2020-09-08
Last Update:	2020-09-08
Current Version:	V1.0
CVSS v3.1 Base Score:	5.3

SUMMARY

The Siveillance Video Client contains an information disclosure vulnerability that could allow an attacker to obtain valid adminstrator login names and use this information to launch further attacks.

Siemens recommends specific countermeasures and provides patches for released versions of the Siveillance Video Client.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Siveillance Video Client: All versions	Apply the patch provided for current versions, available at https://support.industry.siemens.com/cs/ww/en/view/109781490/

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Use Kerberos authentication instead of NTLM as described in the Siveillance Video Hardening Guide

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 CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2020-15785

In environments where Windows NTLM authentication is enabled the affected client application transmits usernames to the server in cleartext.

This could allow an attacker in a privileged network position to obtain valid adminstrator login names and use this information to launch further attacks.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-319: Cleartext Transmission of Sensitive Information

ADDITIONAL INFORMATION

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 (2020-09-08):	Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.