SSA-853866: User Credentials Disclosure Vulnerability in Siveillance Video Open Network Bridge (ONVIF)

Publication Date:	2021-04-13
Last Update:	2021-04-13
Current Version:	V1.0
CVSS v3.1 Base Score:	9.9

SUMMARY

Siemens has released hotfixes for Siveillance Video Open Network Bridge (ONVIF) which fix a security vulnerability related to unsecure storage of ONVIF user credentials. The vulnerability could allow an authenticated remote attacker to retrieve and decrypt all user credentials stored on the ONVIF server.

Siemens recommends to apply the hotfixes at the earliest opportunity. See also the chapter Additional Information, how to apply the hotfix.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Siveillance Video Open Network Bridge: 2020 R3	Apply the hotfix using the latest available installer for Open Network Bridge https://support.industry.siemens.com/cs/ww/en/view/109791980/
Siveillance Video Open Network Bridge: 2020 R2	Apply the hotfix using the latest available installer for ONVIF Bridge https://support.industry.siemens.com/cs/ww/en/view/109781128/
Siveillance Video Open Network Bridge: 2020 R1	Apply the hotfix using the latest available installer for ONVIF Bridge https://support.industry.siemens.com/cs/ww/en/view/109779088/
Siveillance Video Open Network Bridge: 2019 R3	Apply the hotfix using the latest available installer for ONVIF Bridge https://support.industry.siemens.com/cs/ww/en/view/109773456/
Siveillance Video Open Network Bridge: 2019 R2	Apply the hotfix using the latest available installer for ONVIF Bridge https://support.industry.siemens.com/cs/ww/en/view/109769052/
Siveillance Video Open Network Bridge: 2019 R1	Apply the hotfix using the latest available installer for ONVIF Bridge https://support.industry.siemens.com/cs/ww/en/view/109766085/
Siveillance Video Open Network Bridge: 2018 R3	Apply the hotfix using the latest available installer for ONVIF Bridge https://support.industry.siemens.com/cs/ww/en/view/109762643/

Siveillance Video Open Network Bridge: 2018 R2	Apply the hotfix using the latest available installer for ONVIF Bridge https://support.industry.siemens.com/cs/ww/en/view/109762751/

WORKAROUNDS AND MITIGATIONS

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

- Disable the Open Network Bridge (ONVIF), if not in use. Note: By default the Open Network Bridge is disabled.

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.

The Open Network Bridge is an open ONVIF compliant interface for standardized and secure video sharing from Siveillance Video to other IP-based security systems. This enables law enforcement, surveillance centers, or similar organizations (referred to as ONVIF clients) to access live and recorded H.264 video streams from Siveillance Video to their central monitoring solutions.

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-2021-27392

Affected Open Network Bridges store user credentials for the authentication between ONVIF clients and ONVIF server using a hard-coded key. The encrypted credentials can be retrieved via the MIP SDK.

This could allow an authenticated remote attacker to retrieve and decrypt all credentials stored on the ONVIF server.

CVSS v3.1 Base Score	9.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-321: Use of Hard-coded Cryptographic Key

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Milestone PSIRT for reporting and coordinated disclosure

ADDITIONAL INFORMATION

Steps to apply the hotfix:

- Install the VideoOS.OpenNetworkBridge.Installer.exe and follow instructions on screen. You need to update both the ONVIF Plug-in and ONVIF server. Remember to update ONVIF Plug-in on each machine that is running Management Client.
- All previously configured ONVIF users will be removed after applying the hotfix, therefore ONVIF users need to be readded again. To add Open Network Bridge users right click on the tray icon of Open Network Bridge Manager and chose “Manage ONVIF client users. . . ”
- Fill in username and password of an ONVIF user, add the user and apply the settings.

For additional information regarding this vulnerability see the related Milestone Security Advisory.

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 (2021-04-13): 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.