SSA-755517: Path Traversal Vulnerability in Siveillance Video DLNA Server

Publication Date: 2021-11-09
Last Update: 2021-11-09
Current Version: V1.0
CVSS v3.1 Base Score: 8.6

SUMMARY

Siemens has released hotfixes for Siveillance Video DLNA Server, which fix a path traversal vulnerability that could allow an authenticated remote attacker to access sensitive information on the DLNA server.

Siemens has released updates for the DLNA server and recommends to apply the update on all installations where DLNA server used.

AFFECTED PRODUCTS AND SOLUTION

<table>
<thead>
<tr>
<th>Affected Product and Versions</th>
<th>Remediation</th>
</tr>
</thead>
</table>
See further recommendations from section [Workarounds and Mitigations](https://support.industry.siemens.com/cs/ww/en/view/109766085/)

See further recommendations from section [Workarounds and Mitigations](https://support.industry.siemens.com/cs/ww/en/view/109769052/)

See further recommendations from section [Workarounds and Mitigations](https://support.industry.siemens.com/cs/ww/en/view/109773456/)

See further recommendations from section [Workarounds and Mitigations](https://support.industry.siemens.com/cs/ww/en/view/109779088/)

See further recommendations from section [Workarounds and Mitigations](https://support.industry.siemens.com/cs/ww/en/view/109781128/)
Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Disable the DLNA Server, if not in use. Note: By default, the DLNA server is not installed with the other components of Siveillance Video

**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-2021-42021

The affected application contains a path traversal vulnerability that could allow to read arbitrary files on the server that are outside the application’s web document directory.

An unauthenticated remote attacker could exploit this issue to access sensitive information for subsequent attacks.

CVSS v3.1 Base Score 8.6
CWE CWE-26: Path Traversal: ‘/dir/../.filename’

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

• Milestone PSIRT for reporting and coordinated disclosure

ADDITIONAL INFORMATION

For additional information regarding this vulnerability see the related Milestone Security Advisory at https://www.milestonesys.com/support/tools-and-references/cyber-security/.

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 (2021-11-09): 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.