Document ID	Revision	Date	Document category	
AAGS-HOSP-SA-2022-008	**1**	**2022-03-22**	**Security Advisory**	
Confidentiality level			Status	Page (of)
Public			**Approved**	**1 (4)**

AAGS-HOSP-SA-2022-008 – Leakage of Cryptographic Key

Hospitality

TLP:WHITE

Disclosure is not limited.

Overview

A vulnerability has been discovered in Visionline related to information leakage of cryptographic key. The severity is medium.

Advisory Status

Investigation Done

While our product investigation is done, we will continue to monitor the threat environment and update this advisory if this situation changes. Our security teams are actively monitoring our environments and updating our defense-in-depth tools.

AFFECTED PRODUCTS

PRODUCT NAME	VERSIONS
Visionline	Prior to 1.27.0

Document ID	Revision	Date	Document category	
AAGS-HOSP-SA-2022-008	**1**	**2022-03-22**	**Security Advisory**	
Confidentiality level			Status	Page (of)
Public			**Approved**	**2 (4)**

Vulnerability Description

A vulnerability has been discovered in Visionline related to a cryptographic key. Visionline server contains a vulnerability that leaks partial information of an encryption key during certain circumstances. The information leakage reduces the strength of the encryption key.

IMPACT

Using the partial information leakage, a malicious actor could reduce the strength of the cryptographic key.

SEVERITY

The CVSSv3.1 score for this vulnerability is:

CVSS 4.7 (MEDIUM)

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N/E:F/RL:O/RC:C

REMEDIATION

ASSA ABLOY Global Solutions has released a new version of Visionline, which addresses the reported issue. We highly recommend that customers upgrade to Visionline 1.27.0 or later and follow the procedures specified in the upgrade manual for 1.27 (Available on the Service Portal).

We provide mitigation instructions to reduce risks through our support channels before upgrading to Visionline 1.27.0 or later.

Customers who wish to upgrade are recommended to contact their local ASSA ABLOY Global Solutions Office listed in the *Contact Information* section below.

ASSA ABLOY Global Solutions recommends that customers follow appropriate network security best practices such as

- Restricting and segmenting network access to Visionline and its used services
- Monitoring of the network for any signs of intrusions

Specifically, for Visionline network devices and Visionline servers, we recommend that

- Visionline network devices only are used on restricted networks
- Firewalls are recommended to restrict communication to Visionline server and known network devices

CREDIT

Discovered by Timo Hirvonen & Tomi Tuominen from WithSecure

Contact Information

If you have additional questions, don't hesitate to get in touch with us:

- Technical questions for customers with SLA or Service Portal account
  Please raise a case or start a chat session.
  - https://my.assaabloyglobalsolutions.com/assaabloy
- Technical questions for customers without SLA or Service Portal account
  Global Helpdesk: +1 214-833-0797
- Security Advisories updates and security information
  We continuously update our Hospitality Security Resources Center with the latest information related to security concerning our products and services.
  - https://www.assaabloyglobalsolutions.com/en/industries/hospitality/product-security

REFERENCES

ASSA ABLOY Global Solutions Hospitality adheres to a responsible disclosure policy published on our Product Security Center.

The Security Advisories severity level is a self-calculated CVSS score that follows the vulnerability metrics standard.

- https://www.assaabloyglobalsolutions.com/en/industries/hospitality/product-security
- https://www.first.org/cvss/calculator/3.1

REVISION HISTORY

Revision	Date	Description
1. 1	2022-03-22	The initial publication of the advisory

TERMS OF USE

Document ID	Revision	Date	Document category	
AAGS-HOSP-SA-2022-008	**1**	**2022-03-22**	**Security Advisory**	
Confidentiality level			Status	Page (of)
Public			**Approved**	**4 (4)**