Document ID	Revision	Date	Document category	
AAGS-HOSP-SA-2022-005	**1**	**2022-03-22**	**Security Advisory**	
Confidentiality level			Status	Page (of)
Public			**Approved**	**1 (4)**

AAGS-HOSP-SA-2022-005 – No Integrity Check

Hospitality

TLP:WHITE

Disclosure is not limited.

Overview

A vulnerability has been discovered in Visionline related to missing support for integrity check. The severity is high.

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
LCU 6333
LCU 6334
LCU 6351
LCU 5351
LCU 5352

Vulnerability Description

A vulnerability has been discovered in Visionline related to the firmware. The encrypted firmware of the lock is missing support for integrity check.

IMPACT

The firmware does not perform an integrity check on certain activities, which may lead an attacker to make unauthenticated modifications to the lock.

SEVERITY

The CVSSv3.1 score for this vulnerability is:

CVSS 7.0 (HIGH)

CVSS:3.1/AV:P/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/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). Our Visionline firmware 3.x.41.6, included in the 1.27.x release, resolves this issue.

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.

As normal use of the lock does not include performing firmware upgrade (which in turn require physical access and opening of the lock), we recommend to:

- Beware of any suspicious activity, such as signs of tampering of doors or locks.
- Ensure all service personnel is authenticated and from an authorized partner.

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

FITNESS FOR A PARTICULAR PURPOSE. ANY USE OF THE INFORMATION CONTAINED HEREIN OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK. ASSA ABLOY GLOBAL SOLUTIONS RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A STANDALONE COPY OR PARAPHRASE OF THE TEXT OF THIS DOCUMENT THAT OMITS THE DISTRIBUTION URL IS AN UNCONTROLLED COPY. UNCONTROLLED COPIES MAY LACK IMPORTANT INFORMATION OR CONTAIN FACTUAL ERRORS. THE INFORMATION IN THIS DOCUMENT IS INTENDED SOLY FOR END USERS' LAWFUL USE OF ASSA ABLOY GLOBAL SOLUTIONS PRODUCTS.