| Document ID<br>**AAGS-HOSP-SA-2022-009** | Revision<br>**1** | Date<br>**2022-03-22** | Document category<br>**Security Advisory** | |
|---|---|---|---|---|
| Confidentiality level<br>**Public** | | | Status<br>**Approved** | Page (of)<br>**1 (3)** |

# AAGS-HOSP-SA-2022-009 – Remote Code Execution

Hospitality

**TLP:WHITE**

*Disclosure is not limited.*

## Overview

A vulnerability has been discovered in Visionline related to remote code execution. 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 | VERSIONS |
|---|---|
| Visionline | Prior to 1.28.0 |

# Vulnerability Description

An use-after-free vulnerability has been discovered in the Visionline server.

## IMPACT

Successful exploitation of the vulnerability could lead to remote code execution on the Visionline server.

## SEVERITY

The CVSSv3.1 score for this vulnerability is:

**CVSS 7.1 (HIGH)**

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

## REMEDIATION

Full remediation will be available in Visionline 1.28.

Until 1.28 is released, customers are advised to 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

THIS DOCUMENT IS PROVIDED "AS IS". IT DOES NOT IMPLY ANY KIND OF GUARANTEE, WARRANTY, OR UNDERTAKING, NOR DOES IT EXPAND THE SCOPE OF ANY GUARANTEE, WARRANTY OR UNDERTAKING MADE IN ANY AGREEMENT TO WHICH AN ASSA ABLOY GROUP COMPANY IS A PARTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR 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