Document ID	Revision	Seq	Date	Document Category	
D001474628	**1**	8	**2023-11-13**	**Application Note**	
Author				Alternate ID	
Frejd, Jorgen					
Confidentiality Level				Status	Page (of)
PUBLIC				**Approved**	**1 (6)**

Aperio Security Advisory - Best practice for use of Remote Unlock Functionality

Division	**Group Center**
Business Area	**Group Technology Team**
Business Entity	**ASSA ABLOY AB**
Local Business Unit	**Undefined**
Related Projects	
Description	
Revision Note	
Legacy Rev Value 1	
Legacy Rev Value 2	
Owner in PDM	**Frejd, Jorgen**
Document Created	**2023-10-26**
Revision Created	**2023-10-26**
Revision Sequence Created	**2023-10-26**

Table of Contents

Revision History

Revision	Date	Changed by	Description
1	2023-10-26	Jörgen Frejd	Initial Publication

1 Overview

The ASSA ABLOY Aperio platform team have based statements online (Twitter/X) been looking into the Aperio functionality of Remote Unlock and how it can be used.

Link: https://twitter.com/blackflyns/status/1705284432515694720?s=20

The scenarios reviewed revolved around the use of Remote Unlock command from the Access Control Systems and how they may be blocked due to interference or Denial Of Service attacks.

After reviewing the reported issue, we have concluded that a properly coded integration and/or configured installation prevents the effects of the attack listed.

1.1 Advisory Status

The ASSA ABLOY Aperio platform team have concluded an analysis on the Remote Unlock functionality, please see details under the Vulnerability Description.

1.2 Affected Products

The Aperio Remote Unlock functionality is a platform feature which is supported by all Aperio reader products in use with any of the three different Aperio Hub variants (AH20/AH30/AH40).

2 Vulnerability Description

Aperio today has support for Remote Unlock which means that an unlock of the Aperio reader can be initiated as an asynchronous command by the Access Control System instead of being initiated based on an end user presenting a granted credential to the Aperio reader.

When the Remote Unlock command is sent from the Access Control System it is queued in the Aperio Hub until the Aperio reader checks in with the Hub and receives the command and executes the Unlock.

There are two type of commands that can be sent, setDoorMode or grantAccessSequence/doorOpeningCommand from the Access Control System.

setDoorMode
With the setDoorMode command the Aperio Hub will keep track of the intended relock time and when the Aperio reader checks in with the Hub, the unlock time sent to the Aperio reader will be adjusted (decreased) to *ensure the intended relock time*.

grantAccessSequence/doorOpeningCommand
With the grantAccessSequence/doorOpeningCommand command the Aperio Hub will keep the unlock time as is and pass it on to the Aperio reader when it checks in with the Hub, this to *ensure the unlock time.*

The vulnerability suggests that interference or Denial Of Service on the Aperio Wireless Interface would delay the Remote Unlock message reaching the Aperio reader.

2.1 Impact

If interference or Denial Of Service on the Aperio Wireless Interface would occur, worst case the Unlock command would be delayed and be executed by the Aperio reader later at the time which is outside the intended time frame. This will however only be the case if the Aperio system configuration and/or the Access Control System integration towards the Aperio Hub is not done per existing recommendations, see Severity of the finding – according to CVSS 3.1 scoring system:

5.7 (medium)

CVSS v.3 vector:
AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/CR:X/IR:X/AR:X/MAV:A/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X

Remediation for details.

2.2 Severity

Severity of the finding – according to CVSS 3.1 scoring system:

5.7 (medium)

CVSS v.3 vector:
AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/CR:X/IR:X/AR:X/MAV:A/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X

2.3 Remediation

The Aperio platform already have recommendations and features where the stated vulnerability will be eliminated and not a factor.

2.3.1 Recommendations for setDoorMode

setDoorMode should be used with the intended unlock time and not indefinite unlock time. This will ensure that the Aperio reader will not receive an unlock time outside the intended Unlock window. If indefinite Unlock time for some reason is required, a Relock command should be sent at the intended Relock time, this will replace any queued Unlock command in the Hub, thus removing the potential issue.

doorModeNotification should be integrated and used so that setDoorMode commands failing to reach the Aperio reader can be detected. If the doorModeNotification doesn't arrive in the expected time, a cancellation setDoorMode (time set to 0 or resetDoorMode) should be sent from the Access Control System to the Aperio Hub to get back to a known state of the Aperio reader.

2.3.2 Recommendations for grantAccessSequence/doorOpeningCommand

As grantAccessSequence/doorOpeningCommand doesn't expire in the Aperio Hub based on the unlock time, the Time-To-Live setting in the Aperio PAP tool should be used and set to the shortest possible time. This is done in the Remote Unlock configuration for the Hub in the PAP tool.
This will ensure that the command will be removed if it is not consumed by the Aperio reader within the expected time window.

3 Contact Information

Customers with questions about how the Aperio integration works on their particular access control software should consult their software provider.