Document ID	Revision	Date	Document category	
AAGS-HOSP-SA-2026-02	**1**	**March 2026**	**Security Advisory**	
Confidentiality level			Status	Page (of)
PUBLIC			**Approved**	**1 (4)**

Improper Privilege Management

Hospitality

TLP:WHITE

Disclosure is not limited.

Overview

ASSA ABLOY has identified a local security vulnerability in Visionline on Windows systems. Visionline executes a bundled Java runtime from a directory that is writable by all local users by default. Because this executable is launched by a privileged Visionline service, an authenticated local user with server access could replace the executable and cause arbitrary code to run with elevated privileges.

This vulnerability requires local login access to the Visionline server and cannot be exploited remotely.

Document ID	Revision	Date	Document category	
AAGS-HOSP-SA-2026-02	**1**	**March 2026**	**Security Advisory**	
Confidentiality level			Status	Page (of)
PUBLIC			**Approved**	**2 (4)**

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 updated our defence-in-depth tools.

Vulnerability Description

Visionline on Windows uses a bundled Java Runtime Environment located under the system-wide `%ProgramData%` directory:

```
C:\ProgramData\ASSA ABLOY\VisiOnline\webserver\jre\bin\java.exe
```

On Windows systems, the `%ProgramData%` directory inherits default permissions that grant write access to all authenticated users (SID S-1-1-0). As a result, executable files located beneath this directory may be modified or replaced by any local user with login access, unless permissions are explicitly restricted.

Visionline launches this Java executable as part of its normal operation through a privileged service chain.

The observed execution flow is:

1. `%ProgramFiles%\ASSA ABLOY\Visionline\AppWebService.exe`
2. `C:\Windows\System32\cmd.exe /c ""C:\ProgramData\ASSA ABLOY\Visionline\webserver\tomcat\bin\catalina.bat" run"`
3. `C:\ProgramData\ASSA ABLOY\VisiOnline\webserver\jre\bin\java.exe`

The Java process executes under a customer-specific service account which, in observed configurations, is a member of the local Administrators group and runs with high privileges.

An authenticated local user with login access to the Visionline server could replace the Java executable with a modified binary. When the Visionline service is started or restarted, the modified executable would be executed with elevated privileges, allowing arbitrary code execution

Affected Versions

- Visionline versions prior to version 1.34.0 on Windows systems
- Installations where default `%ProgramData%` permissions are in place and not restricted during or after installation

Mitigation Steps

Vingcard recommends that customers take the following actions:

Automatic mitigation

- Upgrade to the latest version that includes this installer fix

Manual mitigation

1. Right-click on the folder `C:\ProgramData\ASSA ABLOY\Visionline\webserver`
2. Select Properties
3. Select the Security tab
4. Click Advanced
5. Click Disable inheritance
6. Select Convert inherited permissions into explicit permissions on this object
7. Remove Users from the list

Vingcard is validating updated installation and hardening guidance to ensure secure file permissions are consistently applied in supported deployments.

Detection

Customers should:

- Review NTFS permissions on Visionline installation directories
- Audit access to `%ProgramData%\ASSA ABLOY\Visionline`
- Monitor file integrity for executable files invoked by Visionline services

Acknowledgements

- Withsecure Exposure Management for informing via responsible disclosure.

Document ID	Revision	Date	Document category	
AAGS-HOSP-SA-2026-02	**1**	**March 2026**	**Security Advisory**	
Confidentiality level **PUBLIC**			Status **Approved**	Page (of) **4 (4)**

REVISION HISTORY

Revision	Date	Description
1		Initial Release

TERMS OF USE