Local Privilege Escalation Due to Writable Executable in Privileged Visionline Service Path

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-3315
State	PUBLISHED
Assigner	NCSC-FI
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-10 18:19:01 UTC
Updated	2026-05-07 20:41:03 UTC
Description	Incorrect Default Permissions, : Execution with Unnecessary Privileges, : Incorrect Permission Assignment for Critical Reso

Risk And Classification

Primary CVSS: v4.0 5.8 MEDIUM from db4dfee8-a97e-4877-bfae-eba6d14a2166

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:U/V:X/RE:L/U:Clear

EPSS: 0.000140000 probability, percentile 0.024910000 (date 2026-05-12)

Problem Types: CWE-250 | CWE-276 | CWE-732 | CWE-276 CWE-276 Incorrect Default Permissions | CWE-250 CWE-250: Execution with Unnecessary Privileges | CWE-732 CWE-732: Incorrect Permission Assignment for Critical Resource

Version	Source	Type	Score	Severity	Vector
4.0	db4dfee8-a97e-4877-bfae-eba6d14a2166	Secondary	5.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L
4.0	CNA	CVSS	5.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

High

Availability

Low

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:U/V:X/RE:L/U:Clear

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Assaabloy	Visionline	All	All	All	All

Operating System	Microsoft	Windows	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ASSA ABLOY	Visionline	affected 1.0 1.33 custom	Windows

References

Reference	Source	Link
www.vingcard.com/en/service-and-support/product-security-center/hospitality-pr...	db4dfee8-a97e-4877-bfae-eba6d14a2166	www.vingcar
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Withsecure Exposure Management (en)

Additional Advisory Data

Workarounds

CNA: * Right-click on the folder C:\ProgramData\ASSA ABLOY\Visionline\webserver * Select Properties * Select the Security tab * Click Advanced * Click Disable inheritance * Select Convert inherited permissions into explicit permissions on this object * Remove Users from the list

There are currently no legacy QID mappings associated with this CVE.