



# Missing XPC Client & NSXPC endpoint validation leads to privilege escalation in Vienna Assistant (MacOS) - Vienna Symphonic Library

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-24068
<b>State</b>	PUBLISHED
<b>Assigner</b>	SEC-VLab
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-26 11:16:20 UTC
<b>Updated</b>	2026-04-03 06:16:06 UTC
<b>Description</b>	The VSL privileged helper does utilize NSXPC for IPC. The implementation of the "shouldAcceptNewConnection" function,

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from ADP

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

**Problem Types:** CWE-306 | CWE-306 CWE-306 Missing authentication for critical function

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**Low**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**High**

Integrity

High

Availability

High

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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Vienna Symphonic Library GmbH</a>	Vienna Assistant	affected 1.2.542	MacOS

#### References

Reference	Source	Link	Tags
<a href="https://seclists.org/fulldisclosure/2026/Apr/3">seclists.org/fulldisclosure/2026/Apr/3</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://seclists.org">seclists.org</a>	
<a href="https://r.sec-consult.com/vsl">r.sec-consult.com/vsl</a>	551230f0-3615-47bd-b7cc-93e92e730bbf	<a href="https://r.sec-consult.com">r.sec-consult.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

#### Vendor Comments And Credit

##### Discovery Credit

**CNA:** Florian Haselsteiner, SEC Consult Vulnerability Lab (en)

#### Additional Advisory Data

##### Solutions

**CNA:** The vendor was unresponsive and did not respond to any of our communication attempts. Therefore, a patch is not available. In case you are using this product, please approach the vendor and demand a fix.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)