



# Local Privilege Escalation via DYLIB Injection in Native Instruments Native Access

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

## Summary

<b>CVE</b>	CVE-2026-24070
<b>State</b>	PUBLISHED
<b>Assigner</b>	SEC-VLab
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-02-02 14:16:35 UTC
<b>Updated</b>	2026-04-29 09:16:23 UTC
<b>Description</b>	During the installation of the Native Access application, a privileged helper `com.native-instruments.NativeAccess.Helper2`

## Risk And Classification

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

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

**EPSS:** 0.000050000 probability, percentile 0.002170000 (date 2026-05-05)

**Problem Types:** CWE-426 | CWE-426 CWE-426 Untrusted Search Path

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

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Application	Native-instruments	Native Access	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Native Instruments	Native Access	affected 3.24 custom	MacOS

#### References

Reference	Source	Link
www.native-instruments.com/en/specials/native-access	551230f0-3615-47bd-b7cc-93e92e730bbf	<a href="http://www.native-instruments.com/en/specials/native-access">www.native-instrum</a>
sec-consult.com/vulnerability-lab/advisory/multiple-vulnerabilities-in-native...	551230f0-3615-47bd-b7cc-93e92e730bbf	<a href="http://sec-consult.com">sec-consult.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

#### Vendor Comments And Credit

##### Discovery Credit

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

#### Additional Advisory Data

##### Solutions

**CNA:** The vendor was unreachable and did not respond to multiple contact attempts. No patch is available. Customers should contact the vendor and request a patch. Update 2026-04-29: The vendor provides a patched version v3.24 fixes the identified security issues.

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

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

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