# Path Traversal Vulnerability in LabOne User Interface

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-6903 |
| **State** | PUBLISHED |
| **Assigner** | NCSC.ch |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-04-23 10:16:18 UTC |
| **Updated** | 2026-04-23 10:16:18 UTC |
| **Description** | The LabOne Web Server, backing the LabOne User Interface, contains insufficient input validation in its file access function |

## Risk And Classification

**Primary CVSS:** v4.0 8.7 HIGH from vulnerability@ncsc.ch

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/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:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-22 | CWE-346 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | CWE-346 CWE-346 Origin Validation Error

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | vulnerability@ncsc.ch | Secondary | 8.7 | HIGH | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X |
| 4.0 | CNA | CVSS | 8.7 | HIGH | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N |
| 3.1 | vulnerability@ncsc.ch | Secondary | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N |
| 3.1 | CNA | CVSS | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/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:X/R:X/V:X/RE:X/U:X

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Zurich Instruments | LabOne | affected 26.01.3.9 custom | Not specified |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| www.zhinst.com/support/download-center | vulnerability@ncsc.ch | www.zhinst.com | |

| | | | |
|---|---|---|---|
| www.zhinst.com/support/security/2026/zi-sa-2026-001 | vulnerability@ncsc.ch | www.zhinst.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

Solutions

**CNA:** Update to LabOne 26.01.3.9 or later. The update can be applied directly through the LabOne software, or downloaded from the Zurich Instruments Download Center at https://www.zhinst.com/support/download-center.

Workarounds

**CNA:** Upgrading to LabOne 26.01.3.9 or later is the only complete remediation. For customers who cannot upgrade immediately, the following workarounds reduce the risk and should be applied together: Against a same-network attacker (an actor on the same network connecting directly to the LabOne Web Server): - Configure a local firewall to limit access to the LabOne Web Server (default port 8006) to localhost only, preventing access from other hosts on the network. - Operate systems running LabOne only within a dedicated, trusted laboratory network that is not connected to the general corporate network or the internet. Against a malicious-website attacker (a user visits an untrusted website while the LabOne Web Server is running, and the website triggers the vulnerable behaviour through the user's browser): - Do not browse untrusted or unknown websites on systems where the LabOne Web Server is active. Where practical, dedicate the LabOne host to instrument control only and avoid general-purpose web browsing on it. Additional risk reduction: For systems that cannot be upgraded, avoiding the storage of credentials, personal data, or sensitive research data on the LabOne host reduces the impact of a successful exploit.

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