# CVE-2026-4433

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-4433 |
| **State** | PUBLISHED |
| **Assigner** | tenable |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-03-24 21:16:29 UTC |
| **Updated** | 2026-04-29 01:00:01 UTC |
| **Description** | An SSH misconfigurations exists in Tenable OT that led to the potential exfiltration of socket, port, and service information v |

## Risk And Classification

**Primary CVSS:** v4.0 1.9 LOW from vulnreport@tenable.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/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-16 | CWE-16 CWE-16: Configuration

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | vulnreport@tenable.com | Secondary | 1.9 | LOW | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E |
| 4.0 | CNA | CVSS | 1.9 | LOW | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Active

Confidentiality

Low

Integrity

Low

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/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

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Tenable Inc. | Tenable Operation Technology | affected 3.18.58 4.2.40 custom | Linux, 64 bit |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| www.tenable.com/security/tns-2026-9 | vulnreport@tenable.com | www.tenable.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:** Tenable has released Tenable OT Security and Tenable OT Security Enterprise Manager ISOs that contains the fix for new installations of the product. The installation files can be obtained from the Tenable Downloads Portal (https://www.tenable.com/downloads/tenable-appliance). Tenable has released the patch to address this issue within the currently deployed products.

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

**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** **status.cve.report**