Junction File Manipulation

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

Summary

CVE	CVE-2026-33694
State	PUBLISHED
Assigner	tenable
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-23 19:17:28 UTC
Updated	2026-04-24 14:50:56 UTC
Description	This vulnerability allows an attacker to create a junction, enabling the deletion of arbitrary files with SYSTEM privileges. As

Risk And Classification

Primary CVSS: v4.0 7.4 HIGH from vulnreport@tenable.com

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

EPSS: 0.000150000 probability, percentile 0.028480000 (date 2026-04-26)

Problem Types: CWE-59 | CWE-59 CWE-59 Improper link resolution before file access ('link following')

Version	Source	Type	Score	Severity	Vector
4.0	vulnreport@tenable.com	Secondary	7.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/I
4.0	CNA	CVSS	7.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/I

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Active

Confidentiality

High

ntegrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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 Nessus Tenable Nessus Agent	affected Nessus Agent 11.1.2 .msi	Windows
CNA	Tenable Inc.	Tenable Nessus Tenable Nessus Agent	affected Nessus 10.11.3 .msi	Windows

References

Reference	Source	Link	Tags
tenable.com/security/tns-2026-13	vulnreport@tenable.com	tenable.com	
tenable.com/security/tns-2026-12	vulnreport@tenable.com	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.

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 registred 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

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