



# CVE-2026-3497

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-3497
<b>State</b>	PUBLISHED
<b>Assigner</b>	canonical
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-12 19:16:19 UTC
<b>Updated</b>	2026-04-16 19:16:34 UTC
<b>Description</b>	Vulnerability in the OpenSSH GSSAPI delta included in various Linux distributions. This vulnerability affects the GSSAPI pa

## Risk And Classification

**Primary CVSS:** v4.0 6.9 MEDIUM from security@ubuntu.com

**CVSS:**4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000350000 probability, percentile 0.101610000 (date 2026-04-16)

**Problem Types:** CWE-908 | CWE-908 CWE-908 Use of Uninitialized Resource

Version	Source	Type	Score	Severity	Vector
4.0	security@ubuntu.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	2.7	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/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/MSX: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	Ubuntu	Openssh	affected 1:10.0p1-5ubuntu5 1:10.0p1-5ubuntu5.1 dpkg	Not specified
CNA	Ubuntu	Openssh	affected 1:9.6p1-3ubuntu13 1:9.6p1-3ubuntu13.15 dpkg	Not specified
CNA	Ubuntu	Openssh	affected 1:8.9p1-3 1:8.9p1-3ubuntu0.14 dpkg	Not specified

### References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/03/18/4	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
lists.debian.org/debian-lts-announce/2026/04/msg00014.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
www.openwall.com/lists/oss-security/2026/03/18/5	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
www.openwall.com/lists/oss-security/2026/03/18/7	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
www.openwall.com/lists/oss-security/2026/03/12/3	security@ubuntu.com	www.openwall.com	
www.openwall.com/lists/oss-security/2026/03/12/3	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
www.openwall.com/lists/oss-security/2026/03/18/2	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
www.openwall.com/lists/oss-security/2026/03/14/4	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
ubuntu.com/security/CVE-2026-3497	security@ubuntu.com	ubuntu.com	
www.openwall.com/lists/oss-security/2026/03/14/3	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

### Vendor Comments And Credit

Discovery Credit

**CNA:** Jeremy Brown (en)

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](#).

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

**CVE.report and Source URL Uptime Status** [status.cve.report](#)