CVE-2026-35387

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-35387
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-02 17:16:27 UTC
Updated	2026-04-02 17:16:27 UTC
Description	OpenSSH before 10.3 can use unintended ECDSA algorithms. Listing of any ECDSA algorithm in PubkeyAcceptedAlgorith

Risk And Classification

Primary CVSS: v3.1 3.1 LOW from cve@mitre.org

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

Problem Types: CWE-670 | CWE-670 CWE-670 Always-Incorrect Control Flow Implementation

Version	Source	Type	Score	Severity	Vector
3.1	cve@mitre.org	Secondary	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenBSD	OpenSSH	affected 10.3 custom	Not specified

References

Reference	Source	Link	Tags
marc.info	cve@mitre.org	marc.info	
www.openssh.org/releasenotes.html	cve@mitre.org	www.openssh.org	
www.openwall.com/lists/oss-security/2026/04/02/3	cve@mitre.org	www.openwall.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.