



# CVE-2026-44405

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

## Summary

<b>CVE</b>	CVE-2026-44405
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 00:16:04 UTC
<b>Updated</b>	2026-05-06 00:16:04 UTC
<b>Description</b>	In Paramiko through 4.0.0 before a448945, rsakey.py allows the SHA-1 algorithm.

## Risk And Classification

**Primary CVSS:** v3.1 3.4 LOW from cve@mitre.org

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

**Problem Types:** CWE-327 | CWE-327 CWE-327 Use of a Broken or Risky Cryptographic Algorithm

Version	Source	Type	Score	Severity	Vector
3.1	cve@mitre.org	Secondary	3.4	LOW	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N
3.1	CNA	CVSS	3.4	LOW	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

Low

Availability

None

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

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Paramiko	Paramiko	affected a4489456b6f65281e172380cc4826cee5e851dbb git	Not specified

## References

Reference	Source	Link	Tags
github.com/paramiko/paramiko/commit/a4489456b6f65281e172380cc4826cee5e85...	cve@mitre.org	<a href="https://github.com">github.com</a>	
ostif.org/wp-content/uploads/2026/05/25-11-2415-REP_paramiko-security-a...	cve@mitre.org	<a href="https://ostif.org">ostif.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)