



# phpseclib has a variable-time HMAC comparison in SSH2::get\_binary\_packet() using != instead of hash\_equals()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-40194
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-10 21:16:27 UTC
<b>Updated</b>	2026-04-10 21:16:27 UTC
<b>Description</b>	phpseclib is a PHP secure communications library. Prior to 3.0.51, 2.0.53, and 1.0.28, phpseclib\Net\SSH2::get_binary_packet() uses != instead of hash_equals() to compare HMACs, which is a variable-time comparison and can be exploited to perform a timing attack.

## Risk And Classification

**Primary CVSS:** v3.1 3.7 LOW from security-advisories@github.com

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

**Problem Types:** CWE-208 | CWE-208 CWE-208: Observable Timing Discrepancy

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**High**

Privileges Required

**None**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**Low**

Integrity

None

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Phpseclib	Phpseclib	affected < 1.0.28	Not specified
CNA	Phpseclib	Phpseclib	affected >= 2.0.0, < 2.0.53	Not specified
CNA	Phpseclib	Phpseclib	affected >= 3.0.0, < 3.0.51	Not specified

### References

Reference	Source	Link	Tags
github.com/phpseclib/phpseclib/releases/tag/3.0.51	security-advisories@github.com	github.com	
github.com/phpseclib/phpseclib/security/advisories/GHSA-r854-jrxh-36qx	security-advisories@github.com	github.com	
github.com/phpseclib/phpseclib/releases/tag/1.0.28	security-advisories@github.com	github.com	
github.com/phpseclib/phpseclib/commit/ffe48b6b1b1af6963327f0a5330e3aa004...	security-advisories@github.com	github.com	
github.com/phpseclib/phpseclib/releases/tag/2.0.53	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

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 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](https://cve.report/api)

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