



# CVE-2021-30130

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

## Summary

<b>CVE</b>	CVE-2021-30130
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-04-06 15:15:00 UTC
<b>Updated</b>	2023-01-27 19:52:00 UTC
<b>Description</b>	phpseclib before 2.0.31 and 3.x before 3.0.7 mishandles RSA PKCS#1 v1.5 signature verification.

## Risk And Classification

**Problem Types:** CWE-347

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Application	<a href="#">Phpseclib</a>	<a href="#">Phpseclib</a>	All	All	All	All

## References

Reference	Source
[SECURITY] [DLA 3198-1] php-phpseclib security update	MLIS
Release 2.0.31 · phpseclib/phpseclib · GitHub	CON
[SECURITY] [DLA 3197-1] phpseclib security update	MLIS
Release 3.0.7 · phpseclib/phpseclib · GitHub	CON
cleanup RSA PKCS#1 v1.5 signature verification (CVE-2021-30130) by terra frost · Pull Request #1635 · phpseclib/phpseclib · GitHub	MISC
CVE Program record	CVE.
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[179459](#) Debian Security Update for phpseclibphp-phpseclib (CVE-2021-30130)

[181232](#) Debian Security Update for php-phpseclib (DLA 3198-1)

[181233](#) Debian Security Update for phpseclib (DLA 3197-1)

© [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](#)