



# CVE-2023-27560

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

## Summary

<b>CVE</b>	CVE-2023-27560
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-03 06:15:00 UTC
<b>Updated</b>	2023-03-10 18:54:00 UTC
<b>Description</b>	Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields.

## Risk And Classification

**Problem Types:** CWE-835

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Phpseclib</a>	<a href="#">Phpseclib</a>	All	All	All	All

## References

Reference	Source	Link	Tags
PrimeField: prevent infinite loop with composite primefields · phpseclib/phpseclib@6298d1c · GitHub	MISC	<a href="#">github.com</a>	
Release 3.0.19 · phpseclib/phpseclib · GitHub	CONFIRM	<a href="#">github.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[182710](#) Debian Security Update for php-phpseclib3 (CVE-2023-27560)

[6000504](#) Debian Security Update for phpseclib (DLA 3749-1)

[6000505](#) Debian Security Update for php-phpseclib (DLA 3750-1)

© [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](#)