



# CVE-2020-23217

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

## Summary

<b>CVE</b>	CVE-2020-23217
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-07-01 21:15:00 UTC
<b>Updated</b>	2021-07-06 12:24:00 UTC
<b>Description</b>	A stored cross site scripting (XSS) vulnerability in phplist 3.5.3 allows attackers to execute arbitrary web scripts or HTML via

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phplist	Phplist	3.5.3	All	All	All

## References

Reference	Source
Bypass Cross Site Scripting Vulnerability on "IMPORT EMAILS" feature in php-list-3.5.4 · Issue #672 · phpList/phplist3 · GitHub	MISC
phpList 3.5.4 released: Security Release   phpList.org	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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)