



# CVE-2018-6520

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

## Summary

<b>CVE</b>	CVE-2018-6520
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-02-02 01:29:00 UTC
<b>Updated</b>	2018-02-15 15:21:00 UTC
<b>Description</b>	SimpleSAMLphp before 1.15.2 allows remote attackers to bypass an open redirect protection mechanism via crafted author

## Risk And Classification

**Problem Types:** CWE-601

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link	Tags
SimpleSAMLphp	CONFIRM	<a href="http://simplesamlphp.org">simplesamlphp.org</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://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, 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)