



CVE-2017-12871

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

Summary

CVE	CVE-2017-12871
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-01 21:29:00 UTC
Updated	2017-09-06 01:36:00 UTC
Description	The aesEncrypt method in lib/SimpleSAML/Utils/Crypto.php in SimpleSAMLphp 1.14.x through 1.14.11 makes it easier for c

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simplesamlphp	Simplesamlphp	1.14.0	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.1	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.10	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.11	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.2	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.3	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.4	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.5	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.6	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.7	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.8	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.9	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.0	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.1	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.10	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.11	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.2	All	All	All

Application	Simplesamlphp	Simplesamlphp	1.14.3	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.4	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.5	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.6	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.7	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.8	All	All	All
Application	Simplesamlphp	Simplesamlphp	1.14.9	All	All	All

References

Reference	Source
Fix an issue with IV generation in SimpleSAML\Utils\Crypto::aesEncryp... · simplesamlphp/simplesamlphp@77df6a9 · GitHub	CONFIRM
SimpleSAMLphp	CONFIRM
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.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](#)