# 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 |

## 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.