# SimpleSAMLphp SOS Fund Audit Fix Log

## Identified Vulnerabilities

### SSP-01-001 XMLSEC: Casting Cryptographic Keys / Signature Bypass (Critical)

Fixed in simplesamlphp/saml2 1.10.5, 2.3.7, 3.1.3, as well as SimpleSAMLphp 1.15.3.

SSPSA 201802-01 / CVE-2018-7644:
https://simplesamlphp.org/security/201802-01
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7644

**VERIFIED**

Cure53: *Fix looks good, verified*

### SSP-01-002 XMLSEC: Various XPath Injections (Medium)

Fixed in https://github.com/robrichards/xmlseclibs/pull/156 **merge pending**
Will be released in **???**

**VERIFIED**

Cure53: *Fix looks good, strict regex, verified*

### SSP-01-003 XMLSEC: DoS in staticLocateKeyInfo (Medium)

Fixed in https://github.com/robrichards/xmlseclibs/pull/155 **merge pending**
Will be released in **???**

**VERIFIED**

Cure53: *Fix looks good, recursion removed, verified*

### SSP-01-004 SAML2: DoS in the Timestamp function (Info)

Fixed in simplesamlphp/saml2 1.10.4, 2.3.5, 3.1.1, as well as SimpleSAMLphp 1.15.2.

SSPSA 201801-01 / CVE-2018-6519:
https://simplesamlphp.org/security/201801-01
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6519

**VERIFIED**

Cure53: *Fix looks good, strict regex, verified*

### SSP-01-005 SimpleSAMLphp: checkURLAllowed can be bypassed (Medium)

Fixed in SimpleSAMLphp 1.15.2.

SSPSA 201801-02 / CVE-2018-6520:
https://simplesamlphp.org/security/201801-02
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6520

**VERIFIED**

Cure53: *Fix looks good, parse_url is adequate, verified*

### SSP-01-006 XMLSEC: Using == For Hash Comparison (Low)

Fixed in https://github.com/robrichards/xmlseclibs/pull/154 and merged.
Will be released in **???**

**VERIFIED**

Cure53: *Excellent one-character fix, looks good, verified :)*

### SSP-01-007 XMLSEC: Dangerous Use of file_get_contents (Low)

Fixed in https://github.com/robrichards/xmlseclibs/pull/153 and merged.
Will be released in **???**

**VERIFIED**

Cure53: *Fix looks good, risky code was removed, verified*

### SSP-01-008 SimpleSAMLphp: Use of UTF8 in SQLAuth (Info)

Fixed in SimpleSAMLphp 1.15.2.

SSPSA 201801-03 / CVE-2018-6521:
https://simplesamlphp.org/security/201801-03
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6521

**VERIFIED**

Cure53: *Perfect, looks good, verified*

### SSP-01-009 SimpleSAMLphp: Potential XSS due to inaccurate URL filtering (Low)

Not deemed as a security issue since the data involved either doesn't originate from user input or is sanitised as a valid HTTP URL.

**WONTFIX**

Cure53: *Fair enough! Cure53 is fine with the resolution*

### SSP-01-010 SimpleSAMLphp: Potential XSS due to missing escaping flags (Low)

Fixed in SimpleSAMLphp 1.15.2, although not deemed as a security issue since the data involved can’t originate from user input (local configuration option in metadata).

**VERIFIED**

Cure53: *Fix looks good, the flags do the trick, verified*