SWAMID Security Advisories

Shibboleth and SimpleSAMLphp Security Advisories

The Shibboleth Consortium publishes security advisories based on the different products at "Identity Provider V3 Security Advisories", Service Provider V3 Security Advisories and the old "Identity Provider V2 and Service Provider V2 Security Advisories".

The SimpleSAMLphp developers publishes security advisories at SimpleSAMLphp Security Advisories.

 Säkerhetshål i Jetty gör att installationer av Shibboleth Identity Provider är sårbara
Pål Axelsson posted on Jun 29, 2018
Shibboelth IdP använder Jetty som applikationsmotor och under senaste tiden har det upptäckts 5 säkerhetsbrister i Jetty[1]. Detta gör att ni som använder Shibboleth IdP inom SWAMID måste uppdatera era installationer av Jetty. Linux- och Windowsinstallationerna av Shibboleth IdP uppdateras med två olika metoder.

Linux

Om ni har använt SWAMID installationsscript för att installera Shibboleth IdP och inte uppdaterat Jetty tidigare kan ni följa instruktionerna på wikisidan Uppgradera Jetty[2], detta gäller även om du installerat på annat sätt men använder Jetty 9.2.x. Om du använder Jetty 9.3.x kan du eventuellt behöva anpassa uppdateringen.

Windows

Hämta hem och installera senaste versionen av Windows installer for Identity Provider 3.3.3[3] och därefter köra installationsprogrammet. Det är endast Jetty som uppdateras om du redan kör senaste version av Shibboleth IdP.

Mer information

1. Jetty Security Announcement, http://dev.eclipse.org/mhonarc/lists/jetty-announce/msg00123.html
2. Uppgradera Jetty, https://wiki.sunet.se/display/SWAMID/Uppgradera+Jetty
3. Windows installer for Identity Provider 3.3.3, https://shibboleth.net/downloads/identity-provider/3.3.3/

- security
- advisory

 Mjukvarubibliotek i SimpleSAMLphp har kritisk sårbarhet runt verifiering av signeringssignaturer
Pål Axelsson posted on Mar 07, 2018
SimpleSAMLphp har skapat en Security Advisory om en sårbarhet i SimpleSAMLphp där det är möjligt att:

- om SImpleSAMLphp är en IdP kan någon som genomför en attack utge sig för att vara en SP och få dess attributrelease eller
- om SmpleSAMLphp är en SP kan någon som genomför en attack totalt lura tjänsten om vem det är om loggar in.

Rekommendationer

Uppgradera till senaste versionen med av det inbyggda verktyget composer genom att köra "composer update".

Mer information

- SimpleSAMLphp Security Advisory 201802-01

- security
- advisory

 Mjukvarubibliotek i Shibboleth SP har sårbarhet runt möjlig dataförfalskning
Pål Axelsson posted on Feb 27, 2018

Shibboleth Consortium har skapat en Security Advisory om en sårbarhet i Shibboleth Service Provider där det är möjligt att genomföra dataförfalskning baserad på felaktig XML.

Rekommendationer

Uppgadera biblioteket XMLTooling-C till V1.6.4 eller senare och starta sedan om påverkade processer (shibd, Apache, etc.).

Hur gör jag detta?

- Linuxinstallationer som använder de officiella RPM-paketen kan uppgradera dessa till senaste versionen för fixen ska installeras.
- MacPORT av Shibboleth SP måste uppdateras från aktuell webbplats.
- Windowsversionen av Shibboleth SP uppgraderas till senaste versionen(V2.6.1.4).

Mer information

- Shibboleth Service Provider Security Advisory [27 February 2018]

- security
- advisory

 Shibboleth version 2 är end-of-life och alla kvarvarande kommer att tas bort 2018-01-31
Pål Axelsson posted on Jan 02, 2018
Den 31 januari 2018 kommer att vara den sista dagen det är möjligt att använda Shibboleth Identity Provider version 2 i SWAMID. Det har då gått 1½ år sedan den blev ”end of life”. Även om det ännu inte har uppstått några kända säkerhetshål anser vi att det är dags att sätta ett sistadatum. Tjänsteleverantörer som använder SWAMID, direkt eller via eduGAIN, sätter sin tillit till att SWAMIDs medlemsorganisationer sköter sin identitetshanteringsmiljö på ett bra och säkert sätt och att då efter 1½ år efter end-of-life fortsätta använda en nyckelkomponent urholkar tilliten.

- security
- advisory

 Shibboleth Identity Provider version 2 end-of-life
Pål Axelsson posted on Jul 31, 2016
As of July 31 2016 Shibboleth Identity Provider is end-of-life. If you still use version 2 please update to the latest version. For more information in Swedish on howto upgrade please see Uppgradera Shibboleth IdP från version 2 till version 3.

- security
- advisory

 Heartbleed
Leif Johansson posted on Apr 11, 2014
OpenSSL används i många system som är anslutna till SWAMID. Detta är SWAMID operations rekommendation av hur heartbleed skall hanteras i SWAMID:

Det finns normalt 2 nycklar i en SP eller IdP: en nyckel för den webserver som utgör användargränssnittet för tjänsten eller IdPn och en nyckel som används mellan IdPer eller SPer. Denna andra nyckel (federationsnyckeln) är den som finns i federationsmetadata. SWAMIDs rekommendation är att dessa nycklar bör vara olika: federationsnyckeln kan med fördel associeras med ett sk självsignerat certifikat som inkluderas i metadata. De som satt upp sin SP eller IdP enligt denna rekommendation behöver normalt inte byta federations-nyckeln utom i följande två fall:

1. En shibboleth idp som uppsatt så att apache hanterar SSL för port 8443 *och* om apache använder en sårbar openssl så bör IdPns federationsnyckel bytas. Förklaringen är att port 8443 använder federationsnyckeln för TLS och om man konfigurerat sin apache att hantera denna port och (tex via ajp) skicka vidare trafiken till shibboleth IdPn så kommer federationsnyckeln att vara tillgänglig för apache-processen och alltså potentiellt blivit exponerad i en heartbleed-attack. Denna port används för SOAP-bindings för AttributeResponse.
2. En simplesamlphp som kör i mod_php så ska den nycklas om oavsett om det är en SP eller IdP om openssl-versionen är sårbar.

Kontrollera på din OS-distributionsleverantörs hemsida om din installerade version av openssl är sårbar. Har du byggt och kompilerat openssl får du själv kontrollera sårbarheten. De versioner av openssl som levererats av openssl är sårbara i version 1.0.1- 1.0.1f och 1.0.2beta

- security
- advisory

Shibboleth Security Advisory - 24 October 2011

Leif Johansson posted on Nov 11, 2011
From http://shibboleth.internet2.edu/secadv/secadv_20111024.txt:

> *A flaw exists in the algorithms specified by the XML Encryption standard that can lead to exposure of personal information under certain circumstances.*
>
> *There is no simple fix for this issue, so deployers are encouraged to consider their use of certain software features and possibly make changes to their configurations if circumstances warrant, as described below.*

The impact for SWAMID is limited since most SPs already use HTTPS. Those SPs that do not today use HTTPS are strongly encouraged to do so as soon as possible.

- security
- advisory