Shibboleth Security Advisory 06/17/2009

An important Security advisory has been announced by internet2. Please make note.

To summarize, a vulnerability has been found in Shibboleth SP software (versions 1.3 and 2.1). This vulnerability was detected in ASP.NET applications running on IIS. The vulnerability is that, once user logs in, clients (browser agents) may be able to spoof the header value of mapped headers (HTTP_REMOTE_USER, HTTP_SHIB_EMAIL etc.).

Check your attribute mapping file (AAP.xml in v1.3 and attribute-map.xml in v2.x) for header names. Check if you are using underscore ("_") or hyphen ("-") in mapped header names. If you are, then you need to patch. We recommend you patch the SP as soon as you can. You may do one of two things:

1. Change attribute mapping in AAP.xml (v1.3) or attribute-map.xml (v2.1 or higher). Do not use underscore ("_") or hyphen ("-") in the mapped header names. For ex, replace SHIB GIVEN NAME with SHIBGIVENNAME; replace SHIB DISPLAY NAME with SHIBDISPLAYNAME.

If you change the mapping please make sure you change the header name in your application as well. If you change the mapping you will need to restart shibd daemon/service.

Or

2. Upgrade the SP software to latest version 2.2. If you are currently on v1.3 configuration will change. If you are on v2.1 or higher it is fairly straightforward. Contact IAMUCLA when you are ready to upgrade.


Attribute mapping looks like this in v2.1. Change "id" as recommended above

```xml
<Attribute name="urn:mace:dir:attribute-def:eduPersonPrincipalName" id="HTTP_SHIB_EPPN">
  <AttributeDecoder xsi:type="ScopedAttributeDecoder"/>
</Attribute>
```

Sample attribute mapping in v1.3. Change "Header" as recommended above

```xml
ATTRIBUTE_RULE NAME="urn:mace:ucla.edu:edimi:attributes:uclaUniversityID"
  CaseSensitive="false" Header="HTTP_SHIB_UID" Alias="uid">
  <AnySite> <AnyValue /> </AnySite>
</ATTRIBUTE_RULE>
```