CVE-2012-5633

----BEGIN PGP SIGNED MESSAGE----
Hash: SHA1

CVE-2012-5633: WSS4JInInterceptor always allows HTTP Get requests from browser

Severity: Critical

Vendor: The Apache Software Foundation

Versions Affected:

This vulnerability affects all versions of Apache CXF prior to 2.5.8, 2.6.5 and 2.7.2. CXF 2.7.1 is not affected by default, however the vulnerability exists if you are explicitly adding the URIMappingInterceptor to the default chain.

Description:

The URIMappingInterceptor in CXF is a legacy interceptor that allows some basic "rest style" access to a simple SOAP service. The functionality provided by this interceptor has since been replaced by the JAX-RS standard.

An example of how this interceptor works is as follows. A simple "double it" webservice is defined as:

```
@WebService(name = "DoubleItPortType")
public interface DoubleItPortType {
@WebMethod(operationName = "DoubleIt")
public int doubleIt(
@WebParam(name = "numberToDouble") int numberToDouble
);
}
```

The URIMappingInterceptor can allow a REST client access the service via a GET request to a URL like:

http://localhost:8080/DoubleItPort/DoubleIt&numberToDouble=20

The vulnerability is when a simple SOAP service is secured with the WSS4JInInterceptor, which enables WS-Security processing of the request. WS-Security processing is completely by-passed in the case of a HTTP GET request, and so access to the service can be enabled by the URIMappingInterceptor.

This is a critical vulnerability if you are using a WS-Security UsernameToken or a SOAP message signature via the WSS4JInInterceptor to authenticate users for a simple SOAP service. Please note that this advisory does not apply if you are using WS-SecurityPolicy to secure the service, as the relevant policies will not be asserted. Also note that this attack is only applicable to relatively simple services that can be mapped to a URI via the URIMappingInterceptor.

This has been fixed in revisions:

http://svn.apache.org/viewvc?view=revision&revision=1409324 http://svn.apache.org/viewvc?view=revision&revision=1420698

Migration:

Although this issue is fixed in CXF 2.5.8, 2.6.5 and 2.7.2, due to a separate security vulnerability (CVE-2013-0239), CXF users should upgrade to the following versions:

Users of CXF prior to 2.5.x should upgrade to either 2.5.9, 2.6.6, or 2.7.3.
CXF 2.5.x users should upgrade to 2.5.9 as soon as possible.
CXF 2.6.x users should upgrade to 2.6.6 as soon as possible.
CXF 2.7.x users should upgrade to 2.7.3 as soon as possible.

References: http://cxf.apache.org/security-advisories.html

----BEGIN PGP SIGNATURE----
Version: GnuPG v1.4.11 (GNU/Linux)

iQEcBAEBAgAGBQJRFM+PAAoJEGe/gLEK1TmDLW8IAKrzgMRi0avREKTbK3xwVcK4
OhpIc2ZckiHjuhTd4CAfR+8MbIIx2aVKTywcIwbvSkwuqAj2YnHrc33RFLA2ifNU
00tKHlDfYWU2MzP+nPPHtgFMQbb9XcIINLeCl8qiJAeZTW3gYOBEQ1XHL7yM1f8E
i3NSyIaIaRHmgB0IDWMNd1pQvkB6OrXJvxPWhkL6ea+GaCaC5+wInQWBWmNUOsj4
m/qnalxDgmRCHSLiHNw6N0l1Qb/nsL45MNvmLQglXZZAR1+npb1jtqega0DchFn7
ohEyVJpkFuASPcPsqeSpSbEYixjXSQCnJvw6RZlOvfXC7F6u49xjrRiskP/RBX0=
=IP0q
----END PGP SIGNATURE----