CVE-2012-3451

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

CVE-2012-3451: Apache CXF is vulnerable to SOAP Action spoofing attacks on Document Literal web services.

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected:

This vulnerability affects all released versions of Apache CXF.

Description:

Each operation in a SOAP web service can be associated with a SOAP Action String (e.g. in the WSDL binding or via an annotation). The web service client can send the SOAP Action String as a header with the request as a way of letting the web service know what operation is required.

In some cases, CXF uses the received SOAP Action to select the correct operation to invoke, and does not check to see that the message body is correct. This can be exploitable to execute a SOAP Action spoofing attack, where an adversary can execute another operation in the web service by sending the corresponding SOAP Action. This attack only works if the different operation takes the same parameter types, and hence has somewhat limited applicability.

This attack also only applies for web services that use unique SOAPActions per service operation which is not the default in CXF. Also note that WS-Policy validation is done against the operation being invoked and thus the incoming message must meet those policy requirements as well, also limiting applicability.

This has been fixed in revision:

http://svn.apache.org/viewvc?view=revision&revision=1368559

All released versions of CXF are affected.

Migration:

Users of CXF prior to 2.4.x should upgrade to either 2.4.9, 2.5.5, or 2.6.2.
CXF 2.4.x users should upgrade to 2.4.9 as soon as possible.
CXF 2.5.x users should upgrade to 2.5.5 as soon as possible.
CXF 2.6.x users should upgrade to 2.6.2 as soon as possible.

References: http://cxf.apache.org/security-advisories.html
----BEGIN PGP SIGNATURE----
Version: GnuPG v1.4.11 (GNU/Linux)

iQEcBAEBAgAGBQJQWeNgAAoJEGe/gLEK1TmD2HYH/AomMsGxr/1WwT9dRQqUROG8
/2DLGe6lF2Ww+BxCxruxRosTU6QciAJqMWyDbIuMq8ANh9lEJNfjd+fxIGque8wo
2nWTc4U/AwLMgBxzonIH4uPDj5HK1R4LGqegzi78/vzJu0F3Q+M7mWPPwLOl6mCg
d0t+PSgWAsi8lVHAd99rxHSOwGnoiDjVjCaSMSpZ/nkYv9giO3YMjf69wKajQmVz
toFBckis8w0GN/GJ52LPPRcHc3ibpRIcPQXPscWdm0jq1b2UYTEwA5ylGMgJw5Lh
VBl8BTGO/dEkuA937UlYu+zUtbRb24RNf9e9eBgzHK32HNoM6zwBgtOf+owjTdM=
=k1gm
----END PGP SIGNATURE----