Apache Wink Security Advisory (CVE-2010-2245)
Apache Wink allows DTD based XML attacks
Author: Mike Rheinheimer (adapted from Axis2, originally by Andreas Veithen)
July 6, 2010

# 1. Description

Apache Wink is vulnerable to DTD based XML attacks. There are two types of such attacks:

- Document type declarations may reference other documents, namely a DTD or external entities declared in the internal subset. If the XML parser is configured with a default entity resolver (which is the case for Wink), this allows an attacker to instruct the parser to access arbitrary files. Since URLs may be used as system IDs, this includes remote resources accessible only in the network where the server is deployed. An attacker may exploit this in several ways:
    - By inspecting the error message in the service response, he may be able to scan for the presence of certain files on the local file system of the server or for the availability of certain network resources accessible to the server.
    - By including an internal subset in the document type declaration of the request and using external entity declarations, he may be able to include the content of arbitrary files (local to the server) in the request. There may be REST services that produce responses that include information from the request message. By carefully crafting the request, the attacker may thus be able to retrieve the content of arbitrary files from the server.
    - Using URLs with the “http” scheme, the attacker may use the vulnerability to let the server execute arbitrary HTTP GET requests and attack other systems that have some form of trust relationship with the Wink server.
- While XML does not allow recursive entity definitions, it does permit nested entity definitions. If a document has very deeply nested entity definitions, parsing that document can result in very high CPU and memory consumption during entity expansion. This produces the potential for Denial of Service attacks.

# 2. Systems affected

## *1.1. Wink deployments*

As shown in section -

[1]

-

# 1.

# 2.

### *1.1.*

# 3.

### *1.2.*

file:///etc/passwd

### *1.3.*

***1.4.***

**4.**

**4.**