CFMX Sandbox Security

Posted At : July 1, 2003 8:09 AM | Posted By : Steven Erat
Related Categories: Java, ColdFusion, Macromedia

Related to my earlier blog referencing Sam and Aaron's demonstration of file access in ColdFusion MX without the use of CFFILE, CFOBJECT, or CreateObject(), there has been a recent discussion on a ColdFusion mailing list that was concerned with potential security breaches as a result of that type of code.

Jochem van Dieten, another very knowledgeable and frequent contributor to ColdFusion lists and forums, has confirmed in his testing that a properly configured server can still restrict file access through this alternate means. Jochem writes:

> Even if somebody can bypass CF MX Sandbox Security (and I am not saying they can), they are still bound by the OS ACLs. So as long as the CF MX Service runs under an account that does not have access to these files there is no way they can be compromised.
> ...
> As long as I don't configure a Sandbox, that code works. As soon as I configure a Sandbox, that code breaks with the following message:
> "java.security.AccessControlException: access denied"
> So apparently a correctly configured Sandbox will not allow the filesystem to be compromised.

A follow-up from Macromedia included:

> It is possible, even with createObject and CFObject disallowed to get access to Java. But, if you have file access and network access restrictions configured in SBS then you will be protected from unauthorized file/network access via Java or CF. Basically, SBS(SandBox Security) creates the same in-memory policy objects that the appserver creates when it loads the java.policy file. When SBS is enabled we start the java.lang.SecurityManager with an unrestricted policy and then using the CF Admin end users can configure these on the fly - I think the CF Admin is much easier to deal with than a Java policy file.

Update 1/28/2004: A Security Patch has been released for this potential vulnerability.