

Crashing any Windows NT TSE running MetaFrame 1.8

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-08/0015.html>

From: morejunkmail@GMX.NET

Date: 08/08/02

Date: Thu, 8 Aug 2002 13:47:04 +0200

From: morejunkmail@GMX.NET

To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

PreScriptum: I posted this at thin-world.community.everyone.net
first.

I tried to contact Citrix about this bug i found, but they warn't interested. (Haven't heard from them.)
So i'm posting it on a public forum for everyone to read.

Any WinNT4 TSE (Terminal Server Edition) running Citrix MetaFrame 1.8 can be brought to its knees using the Java ICA web terminal interface without even logging on the server.

All the required runtime files that are needed to do this are copied to the caching folder of the browser used (eg: IE uses the TemporaryInternetFilesFolder) when accessing a web terminal.

To put it simple: all a hacker/criminal has to do is to create a mirror site (or copy the files from IE cash) of the JAVA ICA environment and make little changes.

The changes are made in the html file that is used to load the "setting" and makes then the ICA session available.

eg:

```
-----  
applet code="com.citrix.JICA.class" archive="jicaeng.jar" width="800"  
height="600"  
-----
```

must be changed to:

```
-----  
applet code="com.citrix.JICA.class" archive="jicaeng.jar" width=100%  
height=100%  
-----
```

NT-Bugtraq: Crashing any Windows NT TSE running MetaFrame 1.8

All a hacker has to do now is to load the HTML file in Internet Explorer then set the browser to fullscreen("F11" key is used in internet Explorer to "FullScreen" the window) and refresh.

At first it may seem that nothing has happened but in fact all connected users are bumped off the server and in most cases the server will "blue screen" and reboot or freeze.

I don't think anyone else has noticed this bug/exploit yet, or citrix would have posted a patch by now.

I have confirmed this bug by testing it on 5 different MetaFrame Servers and they all crashed(!).

Maybe this is a known problem (then I'm an idiot), but I'm pretty sure it's not.

Use this info in peace.
Tanin Ehrami

PS: This mail may be edited for editorial reasons.

--

GMX - Die Kommunikationsplattform im Internet.
<http://www.gmx.net>

- ***Previous message:*** Chris Paget: "White paper: Exploiting the Win32 API."
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]