

# SECURITY ADVISORY

**December 2006**

Citrix "Session Reliability Protocol" Firewall Bypass



## **Table of Contents**

SECURITY ADVISORY .....	1
December 2006 Citrix "Session Reliability Protocol" Firewall Bypass .....	1
Copyright and disclaimer .....	3
The Security Research Team.....	3
Introduction & Advisory Summary .....	3
Credits and Thanks .....	3
Status and Timeline .....	3
What software is affected? .....	4
Primary targets .....	4
Mitigation .....	4
Who can exploit this and where from? .....	4
What is the impact of exploitation? .....	4
CVSS Impact Scores .....	4
CVSS details - Base Metrics (Score: 2.8).....	4
CVSS details - Temporal Metrics (Score: 2.7).....	4
CVSS details - Environmental Metrics (4.3) .....	5
Exploit Details.....	5
What this issue exploits – High-level view .....	5
What this issue exploits – Network traffic view .....	5
Proof-of-Concept Screenshot.....	6

## ***Copyright and disclaimer***

The information in this advisory is Copyright 2006 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.

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 FortConsults Security Research Team lead, Andrew Christensen.

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](http://www.fortconsult.net).

## ***Introduction & Advisory Summary***

What appears to be a design flaw with Citrix's network protocol makes it possible for an outside attacker, without any authentication, to bounce through an enterprise's Citrix server and obtain network access network services behind the firewall, on the Citrix application server (localhost firewall bypass is the only possibility on the most up to date Citrix install we have tested), and possibly on towards other machines which this server can access (this may be possible in older versions).

## ***Credits and Thanks***

Thanks to our customer (a large Danish insurance company, who we will not name here for privacy reasons) for providing access to a nice test-lab full of systems.

## ***Status and Timeline***

December 8<sup>th</sup> 2006

Initial issue discovery

December 21<sup>st</sup> 2006

Citrix Security receives this report via email

## ***What software is affected?***

### **Primary targets**

This issue affects the Citrix Metaframe Server. The specific versions affected are unknown, but the most recent version as of December 1st, 2006 was tested.

### ***Mitigation***

No patch is presently available. It is possible / likely that IDS signatures could be created to recognize attacks in progress, and that host-based firewalls could prevent the vulnerable server from connecting out.

### ***Who can exploit this and where from?***

This can be exploited from the Internet or from internal networks, where TCP port 2598 is visible to the attacker. It appears that this is not an issue in cases where a Citrix Secure Ticketing Authority (STA) controls access through the Session Reliability (XTE) server.

### ***What is the impact of exploitation?***

The attacker will be able to proxy to ports on the Citrix application server (and maybe other systems) behind the victim's firewalls, which are normally not visible from the outside world.

This means that if there is a vulnerable service listening on some port (for example, a vulnerable FTP), but normally only port 2598 is visible, the attacker will be able to bounce through port 2598, in order to attack port 21.

### ***CVSS Impact Scores***

The following scores have been calculated using the online CVSS calculator at <http://www.patchadvisor.com/PatchAdvisor/CVSSCalculator.aspx>

#### **CVSS details - Base Metrics (Score: 2.8)**

Access Vector:	Remote
Access complexity:	High
Authentication:	Not required
Confidentiality Impact:	Complete
Integrity Impact:	None
Availability Impact:	None
Impact Bias:	Confidentiality

#### **CVSS details - Temporal Metrics (Score: 2.7)**

Exploitability:	Functional
Remediation Level:	Unavailable
Report Confidence:	Confirmed

### CVSS details - Environmental Metrics (4.3)

Collateral Damage Potential: Medium

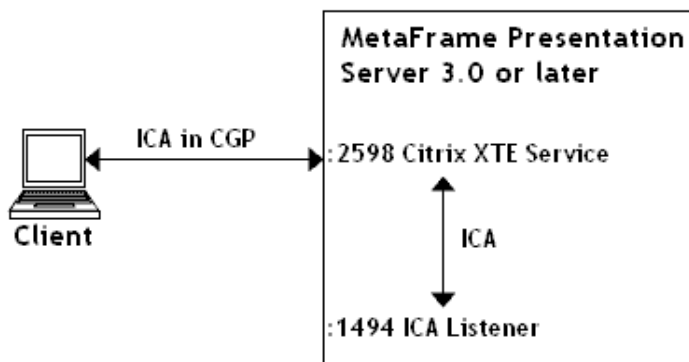
Target Distribution: Medium

### Exploit Details

A Proof-of-Concept Perl proxyserver has been created to exploit this issue. We will consider providing this tool upon written request to [anc@fortconsult.net](mailto:anc@fortconsult.net). A movie created by capturing a VMware session is also available which demonstrates this issue.

### What this issue exploits – High-level view

The “Session Reliability Protocol” is designed to proxy traffic, as shown in the following diagram, taken from <http://support.citrix.com/article/CTX104147>. This Citrix documentation seems to imply that the Session Reliability Server decides where forwarded traffic will be routed; in actuality it seems to be the client which controls the traffic destination:



### What this issue exploits – Network traffic view

Basically, this issue exploits the fact that the Citrix client is allowed to instruct the Citrix Session Reliability server on which host / port to connect to. This can be seen in following network capture hex-dump, which transmits the string “127.0.0.1:1494”. If an attacker replaces that host/port with something else, the server will attempt to proxy a connection to whatever the attacker specified.

Hex-dump of network traffic, as a Perl array:

```
my @conn1 = (
    "\x1e", "\x06", "\x09", "\x01", "\x01", "\x01", "\x00", "\x00",
    "\x00", "\x02", "\x00", "\x00", "\x12", "\x01", "\x0e", "\x31",
    "\x32", "\x37", "\x2e", "\x30", "\x2e", "\x30", "\x2e", "\x31",
    "\x3a", "\x31", "\x34", "\x39", "\x34", "\x03", "\x00" );
```

### ***Proof-of-Concept Screenshot***

In the following screenshot, this issue has been demonstrated by showing a netstat on the Citrix machine, immediately before and right after running the "proxysploit.pl" Perl script, instructing the XTE (Session Reliability Service) to connect to localhost:3389 (Microsoft Remote Desktop Protocol), instead of localhost:1494 (Citrix ICA).

```
Re H:\Desktop>netstat -an | findstr /i "3389"
TCP    0.0.0.0:3389          0.0.0.0:*           LISTENING

I  H:\Desktop>netstat -an | findstr /i "3389"
E  TCP    0.0.0.0:3389          0.0.0.0:*           LISTENING
TCP    127.0.0.1:3389       127.0.0.1:4471      ESTABLISHED
TCP    127.0.0.1:4471      127.0.0.1:3389      ESTABLISHED

H:\Desktop>
```