FORTCONSULT

Straight talk on IT security

SECURITY ADVISORY December 2006

Citrix "Session Reliability Protocol" Firewall Bypass

Discovered in September 2006 by FortConsult's Security Research Team/Andrew Christensen

Table of Contents

Copyright and Disclaimer

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.

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 to any of the systems which the Citrix server can access.

Credits and Thanks

Thanks to our customer (who we do not name here for privacy reasons) for providing access to a nice test-lab full of systems.

Status and Timeline

December 8th 2006	Initial issue discovery

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

What is the impact of exploitation?

The attacker will be able to proxy to ports / systems behind the victim's firewalls, which are normally not visible from the outside world.

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

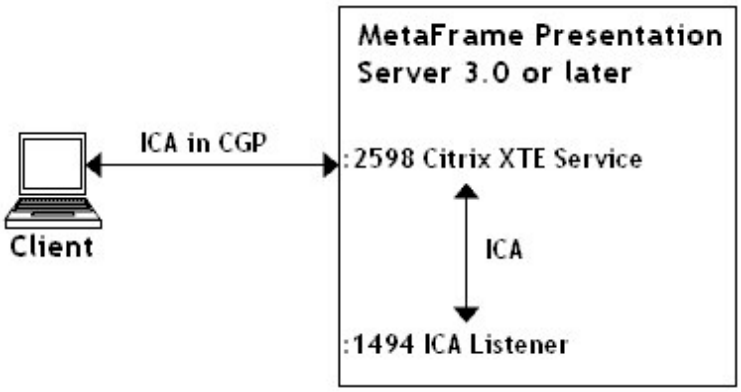
Target Distribution: Medium

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.

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. However, while Citrix documentation seems to imply that the Session Reliability Server decides where forwarded traffic goes, in actuality it seems to be the client which controls the traffic destination:



What this issue exploits – Network traffic view

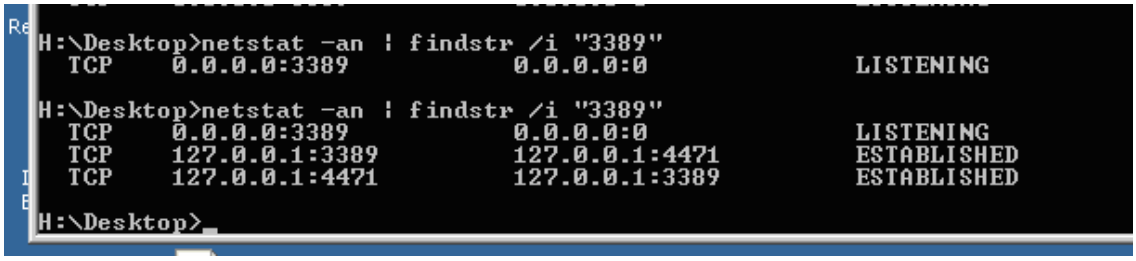
Basically, this issue exploits the fact that the Citrix client is allowed to instruct the Citrix Session Reliability server on which host / port to connect to. This can be seen in following network capture hexdump, which transmits the string "127.0.0.1:1494". If an attacker replaces that host/port with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

Netdump:

```
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).



FORTCONSULT
Straight talk on IT security
FortConsult Tel +45 7020 7525
Tranevej 16-18 Fax +45 7020 7526
DK-2400 Copenhagen NV www.fortconsult.net