

[NT] Citrix Presentation Server IMA Service Invalid Name Length DoS Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-11/msg00009.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 12 Nov 2006 19:14:31 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Citrix Presentation Server IMA Service Invalid Name Length DoS
Vulnerability

SUMMARY

Citrix Presentation Server is a product designed to allow remote access to applications over a network. Remote exploitation of an input validation error in Citrix Systems Inc.'s Metaframe Presentation Server 4.0 IMA service may allow an attacker to cause a denial of service (DoS) condition.

DETAILS

Vulnerable Systems:

* Citrix Presentation Server version 4.0

The IMA (Independent Management Architecture) server component Citrix's Presentation Server (previously known as Metaframe) contains an input validation error in the handling of certain packet types. By constructing a specific packet, it is possible to cause the service to reference an unmapped memory address. This causes an unhandled exception, which in turn causes the service to exit, resulting in a DoS condition.

[NT] Citrix Presentation Server IMA Service Invalid Name Length DoS Vulnerability

Analysis:

Successful exploitation of this vulnerability would allow a remote attacker to cause the IMA server component of the Citrix Presentation Server to crash, preventing access to the resources being shared on the server.

Vendor Response:

The vendor has released the following advisory to address this issue:

<<http://support.citrix.com/article/CTX111186>>

<http://support.citrix.com/article/CTX111186>

Disclosure Timeline:

07/03/2006 – Initial vendor notification

07/05/2006 – Initial vendor response

11/09/2006 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@xxxxxxxxxxxxx>> iDefense Labs Security Advisories.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=441>>

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=441>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.