

[NT] Flash Messaging Server Crash

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0062.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/18/04

To: list@securiteam.com

Date: 18 Oct 2004 10:13:40 +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>

Flash Messaging Server Crash

SUMMARY

<<http://www.flashmessage.com/overview.cfm>> The Flash Messaging System is an "easy to use Network Based Communication Program that runs on all kinds of Windows computers. All PCs on the network are able to send "Popup" messages to each other with the click of the mouse. It is simple, efficient, and has many advanced features."

Due to problems in handling certain input patterns received by clients, the server might crash.

DETAILS

Vulnerable Systems:

* Flash Messaging Server version 5.2.0g (rev 1.1.2)

The network data exchanged between the server and the clients is composed by wide chars (16 bits) and the server is not able to handle some of these chars. The result is the immediate crash of the server.

Another minor issue is that clients may ignore the server's SHUTDOWN command and in fact any other available command. In fact the connection will not be interrupted so the modified clients can continue to stay

Securiteam: [NT] Flash Messaging Server Crash

connected and to chat without problems.

A proof of concept client emulator and data decoder can be found at

<<http://alugi.altervista.org/poc/flashmsg.zip>>

<http://alugi.altervista.org/poc/flashmsg.zip>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:alugi@autistici.org>> Luigi
Auriemma.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.