

[NT] GO-Global Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0039.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/10/05

To: list@securiteam.com

Date: 10 Nov 2005 15:04:38 +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>

GO-Global Buffer Overflow

SUMMARY

<<http://www.graphon.com/products/GO-GlobalforWindows.shtml>> GO-Global for Windows is "a server-based thin-client solution. It allows users to run 32-bit Windows applications remotely from a server, the application runs entirely on the server but is displayed on the client".

A buffer overflow vulnerability exists in GO-Global when initial handshake is done.

DETAILS

Vulnerable Systems:

* GO-Global for Windows versions 3.1.0.3270 and prior

Immune Systems:

* GO-Global for Windows version 3.1.0.3281

After the initial handshake where is specified the type of encryption to use (`_USERSA_`), the application uses 16 bit fields for specifying the length of the subsequent data blocks. Both the client and the server use a small buffer which leads to a buffer-overflow if an attacker uses a data block longer than its size. Both server and clients are vulnerable.

Securiteam: [NT] GO-Global Buffer Overflow

Proof of Concept:

For testing the "GO-Global for Windows" server:

<<http://aluiigi.altervista.org/poc/ggwbof.zip>>
<http://aluiigi.altervista.org/poc/ggwbof.zip>

For testing the "GO-Global for Windows" clients:

<<http://aluiigi.altervista.org/poc/ggwbofc.zip>>
<http://aluiigi.altervista.org/poc/ggwbofc.zip>

ADDITIONAL INFORMATION

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

The original article can be found at:

<<http://aluiigi.altervista.org/adv/ggwbof-adv.txt>>
<http://aluiigi.altervista.org/adv/ggwbof-adv.txt>

=====

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.