

[NT] Buffer Overflows Vulnerability in IglooFTP PRO

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0035.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/08/03

To: list@securiteam.com

Date: 8 Jul 2003 12:17:18 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Buffer Overflows Vulnerability in IglooFTP PRO

SUMMARY

<<http://www.iglooftp.com/windows/index.html>> IglooFTP PRO is "an award winning FTP Client. Its main features are to be easy to use and intuitive when used by novice, but powerful and fully configurable in the hand of experienced users". IglooFTP is vulnerable to a buffer overflow in multiple places (as they all use the same buffer).

DETAILS

Vulnerable systems:

- * IglooFTP PRO version 3.8

Immune systems:

- * IglooFTP PRO version 3.9

By sending a 220 response with a long buffer as the result, it is possible to overflow a local buffer used by the FTP client, allowing a FTP server

Securiteam: [NT] Buffer Overflows Vulnerability in IglooFTP PRO

to cause the client to execute arbitrary code.

A sample buffer would be:

220 [1020 bytes 'A'] [4 bytes EBP] [4 bytes EIP to 'Call ESP']* [41 bytes ShellCode]

ADDITIONAL INFORMATION

The information has been provided by <mailto:peter4020@hotmail.com> Peter Winter-Smith.

=====

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.