

[NT] Glider Collect'n Kill Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0040.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/10/05

To: list@securiteam.com

Date: 10 Nov 2005 15:02:54 +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>

Glider Collect'n Kill Buffer Overflow

SUMMARY

<<http://www.glider-game.com/>> Glider collect'n kill is "a high speed flight shooter developed by <<http://www.revogames.com/>> REVOgames and released at October 2005".

A buffer overflow vulnerability exists in Glider Collect'n Kill game when client sends player name to the server.

DETAILS

Vulnerable Systems:

* Glider Collect'n Kill version 1.0.0.0

A buffer-overflow happens during the copying of the player name sent by the clients with the `gl_playerEnter` command in a buffer of about 4 kilobytes.

Proof of concept:

<<http://aluigi.altervista.org/poc/gliderbof.zip>>

<http://aluigi.altervista.org/poc/gliderbof.zip>

Vendor Status:

Securiteam: [NT] Glider Collect'n Kill Buffer Overflow

No fix.
No reply from the vendor.

ADDITIONAL INFORMATION

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

The original article can be found at:

<<http://aluigi.altervista.org/adv/gliderbof-adv.txt>>

<http://aluigi.altervista.org/adv/gliderbof-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.