

Securiteam: [NT] Limited \secure\ buffer-overflow in some old Monolith games

[NT] Limited \secure\ buffer-overflow in some old Monolith games

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0059.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/17/04

To: list@securiteam.com

Date: 17 Oct 2004 16:23:10 +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>

Limited \secure\ buffer-overflow in some old Monolith games

SUMMARY

<<http://www.lith.com/home.asp>> Monolith is the developer of the famous Lithtech engine. The games affected by the bug were been released before the 2002 but are still played online.

A vulnerability processing a Gamespy 'secure' requests allows a remote attacker to create a buffer overflow condition and crash the client's machine.

DETAILS

Vulnerable Systems:

- * Alien versus Predator 2 Version 1.0.9.6 and lower
- * Blood 2 Version 2.1 and lower
- * No one lives forever Version 1.004 and lower
- * Shogo Version 2.2 and lower

When an attacker sends a \secure\ Gamespy query followed by at least 68 chars a buffer overflow occurs. The limitation of this vulnerability is in the bytes that overwrite the small buffer because only those from 0x20 to 0x7f are allowed while the others are truncated during some internal

steps.

Proof of Concept Code:

A proof of concept code can be found at:
<<http://alugi.altervista.org/poc/lithsec.zip>>
<http://alugi.altervista.org/poc/lithsec.zip>

Solution:

No official fix, probably these games are no longer supported. Luigi Auriemma have received no reply from the developers. Fortunately creating a work-around for this bug is very easy because is only needed to set the "secure" string to NULL.

The following are unofficial patches:

- * <<http://alugi.altervista.org/patches/avp2-1096-fix.zip>> Alien versus Predator 2 – 1.0.9.6
- * <<http://alugi.altervista.org/patches/blood2-21-fix.zip>> Blood 2 – 2.1
- * <<http://alugi.altervista.org/patches/nolf1004-fix.zip>> No one lives forever – 1.004
- * <<http://alugi.altervista.org/patches/shogo22-fix.zip>> Shogo – 2.2

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.