

[NT] Quake 2 Server Format String (Lithium II)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0034.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/08/05

To: list@securiteam.com

Date: 8 Sep 2005 13:49:57 +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>

Quake 2 Server Format String (Lithium II)

SUMMARY

" <<http://www.planetquake.com/lithium/>> Lithium II is a very configurable server-side deathmatch modification for Quake II." By crafting a special nick name it is possible to cause a format string attack under Quake 2 Lithium.

DETAILS

Vulnerable Systems:

- * Quake 2 Lithium II version 1.2

Quake 2 Lithium does not not filter the nick name that users selects for themselves. Creating a nick name such as %999f%f%f%f allow real number to overflow their range and cause a carry flag.

The format string is entered to the stuck as following:

```
004144A1 |. 68 E821AF00 PUSH QUAKE2.00AF21E8 ;
ASCII "0.000000 0.000000 0.000000"
```

The format string takes place when a user is been killed, and the server caused an invalid page fault in module <unknown> at 0000:3030302e.

Securiteam: [NT] Quake 2 Server Format String (Lithium II)

ADDITIONAL INFORMATION

The information has been provided by <mailto:nukemmeister@gmail.com>
sinNULL.

=====

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.