

[NEWS] SCI Photo Chat Server Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0018.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/07/04

To: list@securiteam.com

Date: 7 Jul 2004 16:05:14 +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>

SCI Photo Chat Server Cross Site Scripting

SUMMARY

<<http://www.simmcomm.ch/>> SCI Java Photo Chat Server is "a multithreaded chat server that supports multimedia pictures, sounds, or even videos. It features an integrated HTTP server for transferring images and other media files; a JDBC database interface (tested on PostgreSQL and MySQL) for validating user/password logins; server-side global configuration-file and license management; and more". Due to improper filtering of user provided input third-party content can be inserted in to the product's output, thus attacking visitors to the web server.

DETAILS

Vulnerable Systems:

* SCI Photo Chat Server version 3.4.9

The server does not filter the input strings so they will appear in the returned page. To test the vulnerability:

[http://\[host\]:1235/<script>alert\("hy"\)</script>](http://[host]:1235/<script>alert()

ADDITIONAL INFORMATION

Securiteam: [NEWS] SCI Photo Chat Server Cross Site Scripting

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

The original article can be found at:

<<http://www.autistici.org/fdonato/advisory/SCIPhotoChatServer3.4.9-adv.txt>>
<http://www.autistici.org/fdonato/advisory/SCIPhotoChatServer3.4.9-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.