

[NEWS] Scottrader Unchecked Password Field

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0130.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/23/05

To: list@securiteam.com

Date: 23 May 2005 17:33:58 +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>

Scottrader Unchecked Password Field

SUMMARY

<<http://www.scottrade.com/>> Scottrade, Inc. is "a discount online brokerage firm with over 1.4 million customers. Scottrade began online trading in 1996 and has received high satisfaction ratings since the release of their online trading application called Scottrader".

The Scottrader java applet provides real-time access to market quotes, news services, online ordering, and execution confirmation. Due to an unchecked password field on the server-side, an anonymous user could obtain elevated access to a customer's private account.

DETAILS

The Scottrader Java applet provides an interface to a custom server-side application at Scottrade that provides real-time quote information, account balances, portfolio access, watch lists, orders, order confirmation, news service feeds, and a lot more.

The custom server-side application fails to properly validate new connections, thus allowing an anonymous third party to establish a valid Scottrader connection without the verification of any secret data, password, or other authentication mechanism.

Securiteam: [NEWS] Scottrader Unchecked Password Field

The Scottrader Java applet takes a parameter specified in the HTML page that initiates the applet loading. This parameter is an encoded representation of various account details, including the username and password of the account holder.

The encoding format is easily deciphered by converting the hex string into a byte array and then XOR'ing the bytes with the value 5.

An attacker, armed with the knowledge of a valid account number, can easily start the java applet with the password field NULL or invalid and access any customer account.

Ben Efros is not aware of any pattern to the way account numbers are assigned, but there are a few ways to identify a customer account number:

- Dumpster Dive
- Exploitation of the SCOTTSAVE.COM TRADE HISTORY EXPLOIT
- Random guessing of account numbers (described below)

Guessing account numbers might at first sound near impossible, until you realize that Scottrade identifies all customers with an 8 digit number. Scottrade boasts 1.4 million accounts on their website. Do the math: $1400000 / (9999999 - 1000000) = 0.01555$ The numbers show that you are at least likely to guess right 1.55% of the time.

Vendor status:

Scottrade was contacted January 3rd, 2005. Scottrade was provided vulnerability details the evening of January 24th, 2005.

A coordinated disclosure would have been ideal, but Scottrade has ignored all communications from me since January 24th.

Ben Efros believes enough time has elapsed that the security holes reported have now been corrected.

For more information, contact Scottrade at (800) 619-7283.

ADDITIONAL INFORMATION

The information has been provided by <mailto:befros@gmail.com> Ben Efros.

=====

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.

Securiteam: [NEWS] Scottrader Unchecked Password Field

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.