

[UNIX] SquirrelMail Cross Scripting Attacks (compose.php)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-05/0008.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/02/04

To: list@securiteam.com

Date: 2 May 2004 18:07:14 +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>

SquirrelMail Cross Scripting Attacks (compose.php)

SUMMARY

<<http://www.squirrelmail.org/>> SquirrelMail is "a standards-based web mail package written in PHP4". Multiple cross-site scripting vulnerabilities have been found in the product, these vulnerabilities would allow a remote attacker to steal user cookies (used for authentication).

DETAILS

Vulnerable Systems:

- * SquirrelMail version 1.4.2 and older

Immune Systems:

- * SquirrelMail version 1.4.3 or newer

SquirrelMail is prone to many cross scripting attacks that can be used to steal user cookies. The exploit lies in the way SquirrelMail presents the folder names and shows them.

Example:

Securiteam: [UNIX] SquirrelMail Cross Scripting Attacks (compose.php)

<http://victim.com/mail/src/compose.php?mailbox=INBOX>

Which can be replaced as follows

[<script>malicious script</script>](http://victim.com/mail/src/compose.php?mailbox=)

[<script>window.alert\(document.cookie\)</script>](http://victim.com/mail/src/compose.php?mailbox=)

ADDITIONAL INFORMATION

The information has been provided by <mailto:alvin_gboy@hotmail.com>
Alvin Alex.

=====

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.