

[UNIX] MySQLguest Arbitrary Code Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0021.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/05/04

To: list@securiteam.com

Date: 5 Oct 2004 11:44:35 +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>

MySQLguest Arbitrary Code Injection

SUMMARY

<<http://www.allwebscripts.com>> MySQLguest by "Allwebscripts is a guestbook script that uses MySQL to store messages".

Allwebscripts' MySQLguest is vulnerable to a source code injection vulnerability in the AWSguest.php page. The vulnerability occurs as fields in the AWSguest.php page do not adequately sanitize HTML, script or PHP code.

DETAILS

In the AWSguest.php page, any of the following fields can be used to inject arbitrary HTML, JavaScript or PHP: "Name", "Email", "Homepage" and "Comments".

Exploit:

E-mail: <?php echo <p>Hello World</p>

Homepage: <script language=javascript>alert ("Messagebox")

Comments: <IFRAME SRC=www.computerknights.org>

ADDITIONAL INFORMATION

Securiteam: [UNIX] MySQLguest Arbitrary Code Injection

The information has been provided by BliZZard.

=====

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.