

[NT] Zaep AntiSpam Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-04/0042.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/14/04

To: list@securiteam.com

Date: 14 Apr 2004 09:41:24 +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>

Zaep AntiSpam Cross Site Scripting

SUMMARY

Beyond Security has discovered a security vulnerability in <http://www.zaep.com/> Zaep AntiSpam 2.0, the vulnerability would allow a remote attacker to use the Zaep program's CGI to cause it to return third party content as if it were its own (A cross-site scripting vulnerability). This vulnerability would allow (depending on the web server's configuration and site sensitivity) to steal cookies, display alternative information (cross-site defacement), or redirect users to malicious sites.

DETAILS

Vulnerable Systems:

- * Zaep AntiSpam 2.0

Immune Systems:

- * Zaep AntiSpam 2.0.0.2

Once you send an email to an organization protected by Zaep, a URL like: <http://vulnerable.zaep/?key=3d981f0f.4056b0a6.23285275> is issued. If you modify the URL to include `<script>something</script>`, the Zaep will convert the '/' sign to \, making the script clause not work properly. So

Securiteam: [NT] Zaep AntiSpam Cross Site Scripting

far, this behavior will "protect" the product from a cross-site scripting vulnerability. However, double encoding the / sign (%252F) will bypass this conversion, and allow you to insert malicious content (JavaScript, HTML, etc) into the page.

Exploit (for all the vulnerabilities):

[http://vulnerable.zaep/?key=>alert\(document.cookie\)<%252Fscript>](http://vulnerable.zaep/?key=>alert(document.cookie)<%252Fscript>)

Vendor response:

The vendor has been very cooperative and has issued a patch to redeem this issue as soon as they were notified of this issue (an its severity).

ADDITIONAL INFORMATION

The information has been provided by <mailto:expert@securiteam.com> Noam Rathaus.

=====

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.