

[UNIX] Default CGI.pm Settings Vulnerable to Cross-site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0089.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/21/03

To: list@securiteam.com

Date: 21 Jul 2003 19:04:10 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Default CGI.pm Settings Vulnerable to Cross-site Scripting

SUMMARY

<<http://stein.cshl.org/WWW/software/CGI/>> CGI.pm is "a Perl 5 library that uses objects to create Web fill-out forms on the fly and to parse their contents". A vulnerability in one of the default behaviors of the forms functions, allow remote attackers to cause the CGI.pm to return third-party content that can contain malicious JavaScript/HTML as if it were the CGI's data.

DETAILS

CGI.pm has the ability to create forms by making use of the `start_form()` function. The developer/perl scripter can also makes use of `start_multipart_form()` which relies on `start_form()` and is therefore vulnerable to the same issue. When the action for the form is not specified, it is given the value of `$self->url(-absolute=>1,-path=>1)` - which means that when the URL is something like the following :

Securiteam: [UNIX] Default CGI.pm Settings Vulnerable to Cross-site Scripting

<http://host/script.pl?>">some%20text<!--%20

. the form becomes <form action="<http://host/script.pl>">some text<!-- ">

In such case, it is possible to exploit this issue to launch a Cross Site Scripting attack.

Vulnerable Script Example:

```
#!/usr/bin/perl
# example of exploitable script
#
```

use CGI;

```
$q = new CGI;
print $q->header;
print $q->start_html('CGI.pm XSS');
print $q->start_form();
print $q->end_form();
print $q->end_html;
```

Workaround:

You can bypass CGI.pm's security problem by adding the following code in line 1537 (of CGI.pm):

```
$action =~ s/"/\%22/g;
```

Vendor status:

The vendor was first informed on 30 April 2003. Although the author told EoS that he will be releasing a fix within a week from his last correspondence (May15), no fix is out yet on his website.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:dontreply@eyeonsecurity.org>> obscure.

=====

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.