

[UNIX] ViewCVS's Cross-site Scripting Bug

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0082.html>

From: support@securiteam.com

Date: 05/19/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 19 May 2002 22:00:54 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

ViewCVS's Cross-site Scripting Bug

SUMMARY

<<http://viewcvs.sourceforge.net/>> ViewCVS allows CVS users to browse directories, change logs, and view specific revisions of files that are stored under the CVS engine. Unfortunately, the product has been found to contain a vulnerability that allows for cross-site scripting insertion.

DETAILS

Vulnerable systems:

ViewCVS version 0.9.2 and prior

Proof:

If you access to the URL like;

[http://target_site/cgi-bin/viewcvs.cgi/viewcvs/?cvsroot=>alert\("hello"\)</script>](http://target_site/cgi-bin/viewcvs.cgi/viewcvs/?cvsroot=>alert()

[http://target_site/cgi-bin/viewcvs.cgi/viewcvs/viewcvs/?sortby=rev"><scr!pt>alert\("hello"\)</script>](http://target_site/cgi-bin/viewcvs.cgi/viewcvs/viewcvs/?sortby=rev)

(NOTE, the letter 'i' has been replaced with an '!')

The script code inside the URL will be executed.

(The former URL is valid for Internet Explorer 6.0, Opera 6.01, but not valid for Netscape 4.78, Netscape 6.2.2, Mozilla 0.9.9 on windows XP.)

Securiteam: [UNIX] ViewCVS's Cross-site Scripting Bug

Vendor status:

Vendors are noticed at 13 Mar 2002, and 26 Mar 2002.

Unofficial patches:

The following are two unofficial patches:

* One was made by <mailto:kenji@po.gansekine.jp> Kenji Suzuki / Hyper NIKKI System Project (<http://www.h14m.org/>).

```
--- viewcvs.py.orig Fri Dec 14 23:14:39 2001
+++ viewcvs.py Sun Mar 31 15:24:34 2002
@@ -172,7 +172,7 @@
     # parse the query params into a dictionary (and use defaults)
     query_dict = default_settings.copy()
     for name, values in cgi.parse().items():
- query_dict[name] = values[0]
+ query_dict[name] = cgi.escape(values[0])

     # set up query strings, prefixed by question marks and ampersands
     query = sticky_query(query_dict)
```

The other was made by <mailto:tach@sourceforge.jp> Taku YASUI / Sourceforge.jp (<http://sourceforge.jp/>)

```
=====
RCS file: /cvsroot/viewcvs/viewcvs/lib/viewcvs.py,v
retrieving revision 1.107
retrieving revision 1.108
diff -u -r1.107 -r1.108
--- viewcvs/viewcvs/lib/viewcvs.py 2002/02/22 09:20:46 1.107
+++ viewcvs/viewcvs/lib/viewcvs.py 2002/04/01 01:32:16 1.108
@@ -180,8 +180,14 @@

     # parse the query params into a dictionary (and use defaults)
     query_dict = default_settings.copy()
+
+ # RE that ViewCVS doesn't use in any URL, but a CSS attack might
+ re_url_validate = re.compile("\\|<|>")
     for name, values in cgi.parse().items():
- query_dict[name] = values[0]
+ # do not accept values that contain non-ViewCVS characters
+ # except for search
+ if not re.search(re_url_validate, values[0]) or name == 'search':
+ query_dict[name] = values[0]

     # set up query strings, prefixed by question marks and ampersands
     query = sticky_query(query_dict)
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:office@office.ac> office.

Securiteam: [UNIX] ViewCVS's Cross-site Scripting Bug

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] More than Fourteen CGIscript.net Scripts Have Path Disclosure Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)