

[UNIX] CSVForm (Perl CGI) Remote Execution Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0053.html>

From: support@securiteam.com

Date: 12/14/01

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 14 Dec 2001 16:13:35 +0100 (CET)

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.

CSVForm (Perl CGI) Remote Execution Vulnerability

SUMMARY

<<http://www.ezscripting.com/scripts/csvform1.html>> CSVForm is a Perl script designed to add records to a CSV database file. A security vulnerability in the product allows attackers to cause the program to execute arbitrary code.

DETAILS

Vulnerable systems:

CSVForm.pl v0.1 (and possibly CSVFormPlus)

This script does not appear to be actively maintained yet it does appear to be used on a number of web sites. Unfortunately, for those who adhere to the author's request to notify him of its use, they may be particularly vulnerable if they happen to be listed under the "Check out sites using our scripts" link located on the homepage.

Problem description:

Examining the script shows that after the query is parsed and the parameter of file is obtained, it is passed directly to the following code sample unfiltered.

Securiteam: [UNIX] CSVForm (Perl CGI) Remote Execution Vulnerability

```
sub modify_CSV
{
if(open(CSV,$_[0])){
}
else{
    goto &produce_error(
        "Can't open CSV file.\n",
        "Please, check that you have provided the cgi script with
correct CSV file",
        " path in the HTML form.\n"
    );
}
}
```

Exploit:

http://server/cgi-bin/csvform.pl?file=COMMAND_GOES_HERE%00

Workaround:

Hardcode path to CSV data file or apply proper input validation.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jgomes@strataone.com>> Jason Gomes.

=====

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: "[NEWS] "Spammers Delights" (Mailto.exe)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)