

[UNIX] AWHTTPd Local DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0022.html>

From: support@securiteam.com

Date: 01/05/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 5 Jan 2002 20:38:56 +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.

AWHTTPd Local DoS

SUMMARY

<<http://hardcoresoftware.cjb.net/awhttpd/>> AWHTTPd is a small web server application.

Local users with access to the HTTP directory can cause a denial of service attack against the product.

DETAILS

Vulnerable systems:

AWHTTPd 2.2 and earlier versions

Any local user with write access to awhttpd's html directory can crash the daemon by crafting a special script which is parsed by awhttpd's scripting engine (this is enabled by default). The offending code exists on line 29 of misc.c:

```
if (filefd[i] != (FILE *) -1) fclose(filefd[i]);
```

Example:

A sample awhttpd script follows:

```
# test.cgi
```

```
---AWHTTPD SCRIPT---
```

```
echo "this is a test"
```

Securiteam: [UNIX] AWHTTPd Local DoS

F:test.html

If test.html doesn't exist in the html directory, awhttpd will crash on the fclose().

Fix:

Apply the patches below or disable the scripting engine by editing config.h in the root source directory of awhttpd.

```
=====[ begin cut here ]=====  
--- misc.c.orig Wed Jan 2 16:22:24 2002  
+++ misc.c Wed Jan 2 16:26:37 2002  
@@ -26,7 +26,7 @@
```

```
void discon(int i) {  
    close(infd[i]);  
- if (filefd[i] != (FILE *) -1) fclose(filefd[i]);  
+ if (filefd[i] != NULL) fclose(filefd[i]);  
    if (sending[i] > 0) numofusers--;  
    sending[i] = 0;  
    getreqs[i][0] = 0;  
=====[ end of misc.c patch ]=====
```

```
=====[ begin cut here ]=====  
--- procsrpt.c.orig Wed Jan 2 16:27:33 2002  
+++ procsrpt.c Wed Jan 2 16:51:47 2002  
@@ -38,6 +38,12 @@  
    sending[i] = 1;  
    strcpy(getreqs[i], tdbuf+2);  
    stripctrlf(getreqs[i]);  
+ if (doesfileexist(getreqs[i]) == 0) {  
+ strcpy(tdbuf, "Error: cannot locate ");  
+ strncat(tdbuf, getreqs[i], 256);  
+ strcat(tdbuf, " for reading!\n");  
+ logthis(3, tdbuf);  
+ }  
    fclose(filefd[i]);  
} else if (tdbuf[0] == 0) {  
    discon(i);  
=====[ end of procsrpt.c patch ]=====
```

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:methodic@slartibartfast.angrypacket.com>> methodic.

=====

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

Securiteam: [UNIX] AWHTTPd Local DoS

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: "[EXPL] Solaris /bin/login Remote Exploit Code"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)