

[UNIX] Webmin Insecure Temporary File Creation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0065.html>

From: support@securiteam.com

Date: 10/23/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [UNIX] Webmin Insecure Temporary File Creation

Message-Id: <20011023071731.B44F3138BF@mail.der-keiler.de>

Date: Tue, 23 Oct 2001 09:17:31 +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.

Webmin Insecure Temporary File Creation

SUMMARY

<<http://www.webmin.com/webmin/>> Webmin is a web-based interface for UNIX system administration. Using any browser that supports tables and forms (and Java for the File Manager module) you can setup user accounts, Apache, DNS, file sharing and so on. A security vulnerability in the product allows users with local access to gain administrative privileges.

DETAILS

Vulnerable systems:

Webmin version 0.80

Webmin version 0.88

Webmin creates temporary insecure files in '/tmp' directory, those file are -rwxrwxrwx (777) and owned by root. This means that anyone can modify the file during its execution and add additional commands that will be executed by the root. This is a way to gain root privileges, to create files, modify files, etc.

Example:

Simply add 'cp /bin/sh /tmp/.backdoor' at the end of the file and it will

Securiteam: [UNIX] Webmin Insecure Temporary File Creation

be executed, giving you a root shell in the /tmp directory.

Fix:

The problem is located in the script run.cgi that creates the temporary file giving it bad permissions.

```
-----  
$temp = &tempname();  
open(TEMP,">$temp");  
..blabla...  
chmod(0777, $temp);  
-----
```

To fix, change the line:

```
chmod(0777, $temp);  
to  
chmod(0700, $temp);
```

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:aurelien.cabazon@isecurelabs.com>> Cabazon Aurelien.

=====
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] Network Query Tool Command Execution Vulnerability"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)