

[UNIX] Apache Mis-configuration Can Make You Vulnerable to a Local Denial of Service Attack

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0070.html>

From: support@securiteam.com

Date: 01/15/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 15 Jan 2002 09:49:56 +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.

Apache Mis-configuration Can Make You Vulnerable to a Local Denial of Service Attack

SUMMARY

A common mis-configuration can occur within major ASP/Hosting sites, whereas a remote hosting administrator is allowed access to its logging directories with write access. This would open up the server to a local denial of service, since Apache will not start if one of its logging directories is missing, or cannot be accessed.

DETAILS

The problem occurs when the log directory does not exist, when Apache receives, a SIGHUP (e.g. when logrotate runs) Apache will reload its configuration file and shutdown immediately. Therefore, if the log directory is removed by the owner of the domain by accident or because he just wanted to clean up some logs, apache will just simply shutdown upon a SIGHUP.

Vendor response:

The documentation explicitly states that you must not allow non-trusted users write access to the logs directory. It is a major security hole because they are opened by the user that starts Apache (normally user

Securiteam: [UNIX] Apache Mis-configuration Can Make You Vulnerable to a Local Denial of Service Attack

root). This is done on purpose, however it requires that the server to be misconfigured. If you have a setup where a random user can write to the logs directory, then you have a lot more to worry about than they causing the server to not start.

Having a non-existent log directory is considered a major configuration error, and it is not appropriate for Apache to blindly continue on trying to guess what it should do (and possibly not logging anything).

Also, note that it is not only missing log directories that will cause Apache to fail to startup correctly, but there are a number of major configuration errors that will cause it to do the same thing.

ADDITIONAL INFORMATION

The information has been provided by <mailto:tozz@embrace.selwerd.nl>
Tozz and <mailto:marcs@znep.com> Marc Slemko.

=====

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: "[NT] EServ Password Protected File Arbitrary Read Access Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)