INFORMATION SECURITY

How can log poisoning be successful with a Local File Inclusion attack?

Asked 9 years, 2 months ago Active 9 years, 2 months ago Viewed 7k times

2

I just read a paper about Local File Inclusion on exploit-db.com, it can be found here. One technique with LFI is log poisoning as you may know already. You do an HTTP GET request that contains PHP code. Since it's not a correct HTTP request it gets logged in the apache error.log. Now the attacker can execute the PHP code within the error.log by doing something like http://victim.com/include.php?file=../../../../var/log/apache2/error.log. Now what I don't understand is thefollowing: logs by default are not world readable, so www-data who owns the apache2 process is not able to read error.log and so cannot execute the code within it! How can a log poisoning attack be successful then??

2

web-application attacks linux webserver php

Share Improve this question Follow

asked Jan 26 '12 at 23:42

JohnnyFromBF

1,373 4 15 23

Obviously, logs have to be `www-data` -readable. – Mischa Arefiev Jan 27 '12 at 8:45

1 Answer

Active Oldest Votes

Perfectly legal and smart attack.

5

You're question really boils down to "how does this work when logs are by default not readable by the webserver?".

The fact is that many webservers are set up with custom log directories where the access control is not necessary enforced. This happesn more often than you would think. In some cases the access control for the log files is wide open because sysadmin needed some other system to read them, and he just opened it up for all processes.

This can also be used to execute code from other log files like from the SSH auth log. More on this here: http://lanmaster53.com/2011/05/local-file-inclusion-to-remote-command-execution-using-ssh/

Basically it boils down to wrong permissions on the files. Even so its a good attack which is very relevant.

Share Improve this answer

Follow

edited Jan 27 '12 at 13:17

answered Jan 27 '12 at 12:51

Chris Dale

15.9k 10 53 97

This attack is demonstrated by me on Youtube: youtube.com/watch?v=jEU8w3h1u1o – Chris Dale Mar 17 '14 at 11:17