Vinci Nicolò

Pathname Attacks

08/10/2021

Security flaw and patches:

The flaw regards the body parameter of the post request performed by a user to memo.cgi application. The parameter is used to build an absolute path to recover a memo. However, a user can move freely through the directory manipulating the parameter injecting "**../**". Moreover, memo.cgi is executed with SUID-root permission, so a user can also access to root directories and files such as /etc/shadow. Hence, there are two problems:

1. There is no input validation of the body parameter.
2. The memo.cgi script runs as root due to the SUID-root permission. So, also the memo.pl script runs as root, because it is called by the memo.cgi.

First of all, an input validation has been added into memo.pl script. It checks the presence of "**..**" in the parameter with the following if statement:

```
if ($memo =~ m#^[a-zA-Z0-9_\/]*\.\.[a-zA-Z0-9_\/\.]*$#)
```

Then, if the parameter is able to pass this check, it will also be sanitized with the Perl function abs_path(). This redundancy is to assure the absence of path traversal attack.

After that, memo.cgi has been removed and memo.pl has been renamed as memo.cgi. In this way, the oldest memo.pl will run with non-root permission. The last operation has been performed manually on the machine.

Recovery plan:

The breach was really serious, because a malicious user could move freely in any directory and file of the machine with root permission. So, he could retrieve sensible data such as the hashed passwords of any user in the shadow file. The mitigations described above should be applied to secure the server. Any password should be reset in case of leak of the shadow file.

Explanation:

It is not enough to check that any pathname starts with "/home/username/memo" or "/root/memo/", because a user can go up directories simply by injecting "**../**". When the user reaches the initial folder, he can build any path towards any directory. So, he can access any file in the machine especially if he has root privileges.

Alternative design:

An alternative design may be to remove the memo.cgi script and rename the memo.pl script in "memo.cgi". So, the new memo.cgi script does not run with root privilege anymore. Another way, it may be to remove the SUID-root permission to the actual memo.cgi script, giving to it only the plain executable permission.