To: William H. Flathead III

From: Claudio Facchinetti

Subject: Security issue: Pathname attack

Date: October 3, 2021

The objective of this memo is bring to your attention a security issue that has been discovered in one of the company systems: the memo service.
As you probably know this service is exposed via the URL `/cgi-bin/memo.cgi` on our server. This page presents a serious security vulnerability which allows any attacker to be able to access and read any file on the server by exploiting a vulnerability known with the name of "path traversal".
The problem lies in the dropdown menu which allows a user to select memo to read: using a normal web browser it is possible to edit the page and change the memo requested to any file; moreover an attacker could do the same without using a browser but simply issuing an HTTP request to that page requesting a particoular file.
Exploiting this vulnerability an attacker could pass `/etc/shadow` as path to be read and would gain access to an extremely important file, or basically to any file on the server that he could think about.
I also noticed that the `memo.cgi` executable is just a wrapper used to call the `memo.pl` file using SUID-root permissions, which is quite harmful; I have already proceeded to fix the problems I just reported to you.
As a first thing I removed the SUID-root permissions: I deleted the `memo.cgi` file and renamed `memo.pl` to `memo.cgi`, so that there will be no service disruptions and the service no longer runs with SUID-root permissions.
As a second thing I edited to perform the following fixes on the `memo.cgi` file so that the requested file path is firstly resolved into an absolute path and get retrieved if and only if it relies in the `memo` folder inside a user home directory or inside the `/root/memo` folder.
As a further remark I would like to add that simply performing the latter check without resolving first the path would not fix the vulnerability of path traversal: in Unix file systems there is a special notation to target the parent directory, which is `..` (two dots).
If only the latter check is implemented then an attacker could read any file the script executed without SUID-root permission has access: an attacker requesting
/home/barbazzo/memo/../user_account_reminder would read the *user_account_reminder* file even if it is not intended to be available.
As an additional security measure it is mandatory to change the password of all users having an account on our server and it would be better to track down any suspicious access happened on the company systems since the memo service has been made available.
Concluding the memo I would like to say that this security issue has now bees solved employing the security restrictions just discussed, however it is impossible to retrieve any data about how much and which data has been subtracted to the company and it could have been used.