

Forum:[Hack Forums](#)

Thread: [Hacking cPanel With ~/.contactemail - Resetting Passwords](#)

Hackers - January 7, 2024, 6:58 am

This tutorial is based on how one of my old servers was compromised. It took nearly 2 years to figure out how the hacker was repeatedly re-gaining access to a cPanel account. This is something that may even be patched in the newest cPanel licenses, but there are reports going all the way into 2022 and 1 report in 2023 of the hack still around. Older versions are obviously much more vulnerable.

The whole hack is centered around cPanel's method of storing contact emails for users in plaintext in a file:

Code `~/.contactemail`

TLDR Version:

- update `.contactemail` to have any email address
- using cPanel reset password will now send the password reset link to the new email address, instead of original email on file
- because `.contactemail` has not always been secure, many servers are vulnerable
- any vulnerability that allows a hacker to edit files, even if the hack is 100% unrelated to cPanel, can be used to edit `.contactemail` for this method

Although the emails of users are tracked elsewhere as well, this file can be manipulated to take control. For example, WHCMS has a list of users with a variable in each file for `CONTACTEMAIL`, but when updates roll out this just replaces the value inside the individual `.contactemail` file, per user. However, if you change the value in `.contactemail`, parts of cPanel use that without doublechecking other values in the master list. What this means is that if you can write to `.contactemail`, you can get full control of the cPanel.

The reason this is bad is because `contactemail` was not readonly / secured by default. For example, we brought on a new client that had an infected Wordpress. because the hacker was already in there, they were already targeting the email file. Any time we locked them back out, they were still able to get back in. This is because we would change password, even change the email ourselves, and also alter permissions for files on the system, and remove their PHP shells... but we didn't know about `contactemail`.

You see, once you have access to the system and have found the `.contactemail` file, you have a few options, and this is what the hacker did to us:

Spoiler [\(Click to View\)](#)

1:

- modify `.contactemail` directly, allowing you to change the email assigned to the cPanel account
- use the default cPanel reset password, which sends a reset email to the new email in the `.contactemail` file. The hacker could change password to anything they wanted and put everything they needed back in place.

2:

- because multiple Wordpress installs were infected by the same hacker, and we had a few of them on our servers, we were able to catch a few slick tricks. One of them was a symlink between another file and `.contactemail`
- We're not sure if they had to use this, but it actually was the first major hint that helped us discover

the hack. Because we knew it was weird to see a symlink between a hidden file and another, we were able to investigate and come across others who had this bug in their cPanel installs (unsecure .contactemail file being abused by a hacker).

- The symlink method is interesting because theoretically the hacker could be locked out of this area of the server, but possibly still update it from another place depending on user permissions for the server.

In our case, the hacker used the AnonymousFox hacks originally to infiltrate Wordpress. We're not sure what else they did, but once in they used this exploit very, very well. The reason it went so well is because for literally almost 2 years it was a game of cat & mouse. We locked it down, they broke in. We hunted, they hid. Because the .contactemail is a default file of cPanel, and hidden too, we weren't detecting the file changes to it. We were looking for other files changes by using checksums, file modified dates, etc. For example, if they uploaded a new .php file, we would've detected it and closed it down - if their scripts tried to upload files, we could detect that. What we could not detect because we did not anticipate it was them changing the value of .contactemail, resetting it using normal methods, and then logging in and using normal filemanager to edit files via cPanel...
Lessons learned!

Again - this is much more of a hack for older versions of cPanel, but I do see some recent notes on it that suggest it's either not fully patched, can be manipulated depending on server settings, or there simply are a lot of people still using older cPanel versions. Either way, this was the worst any of my servers ever got hacked and I am happy to share this info if it helps you complete your own pentesting or to otherwise secure your server.

Scofield112 - January 12, 2024, 7:08 pm

so fucking gooooooooooooooouuuuuuuuuuuuuuuuuuuuuuuuu [warn]

xanutree - January 19, 2024, 4:48 pm

there are any way to secure cPanel? how to disable or restrict contactmail file?

Hackers - January 19, 2024, 4:56 pm

(Jan 19, 2024 05:48 PM)xanutree Wrote: [\[CITE\]](#) there are any way to secure cPanel? how to disable or restrict contactemail file?

Chmod, chown, protect against directory traversal code, don't let your server get infected

MarkGold - January 20, 2024, 4:20 am

thank you for this useful tut hope to see more content fro myou

Hackers - January 31, 2024, 5:37 am

(Jan 20, 2024 05:20 AM)MarkGold Wrote: [CITE](#) thank you for this useful tut hope to see more content fro myou

Thanks Mark, I plan on releasing more tutorials over time. Glad you found this useful!