

Forum:[Hack Forums](#)

Thread: [can someone help me with this EXIM exploits? thx](#)

SIM-5137958 - January 13, 2022, 1:52 am

i am learning hacking and currently studying how to exploit via this vulnerability:
CVE-2020-28018

i tried to send command "RCPT TO <...>" command by python, however an error come up and says AUTH is required when send emails on port 587

does that mean, my website won't be vulnerable to CVE-2020-28018 if the attacker doesn't know the credentials to login to my site?

Skorp - January 13, 2022, 2:47 am

This is a cool little exploit used while back on some targets!

For starters, what is your EXIM version, you might want to confirm if it is indeed vulnerable (ofcourse no patch aswell) and another thing I would check is your TLS config. Ofcourse making sure it is enabled.

Also when you check, make sure pipelining is enabled (sync) with TLS. Specifically to this exploit, the first thing it does "when checking" is that it sets up the channel for TLS to your target. If it doesn't connect or nothing gets sent out, it will throw a 200 (which you may be getting). It is very important that you make sure and verify your TLS is setup so it can tunnel through. If it is not enabled correctly, your target will not be exploitable! Making sure everything is setup correctly won't trigger any false positives and should give you the results you were looking for.

Importantly, I personally changed and made my own command from inject_cfg and did a modified netcat reverse shell so you may want to change yours to your liking if you are still running into issues with whatever your checking mail variable is. Goodluck man! Hope it works out for you! ^.^

4.90 -> 4.94.X

SIM-5137958 - January 13, 2022, 3:23 am

(Jan 13, 2022 03:47 AM)Skorp Wrote: [\[CITE\]](#) This is a cool little exploit used while back on some targets!

For starters, what is your EXIM version, you might want to confirm if it is indeed vulnerable (ofcourse no patch aswell) and another thing I would check is your TLS config. Ofcourse making sure it is enabled.

Also when you check, make sure pipelining is enabled (sync) with TLS. Specifically to this exploit, the first thing it does "when checking" is that it sets up the channel for TLS to your target. If it doesn't connect or nothing gets sent out, it will throw a 200 (which you may be getting). It is very important that you make sure and verify your TLS is setup so it can tunnel through. If it is not enabled correctly, your target will not be exploitable! Making sure everything is setup correctly won't trigger any false positives and should give you the results you were looking for.

Importantly, I personally changed and made my own command from inject_cfg and did a modified

netcat reverse shell so you may want to change yours to your liking if you are still running into issues with whatever your checking mail variable is. Goodluck man! Hope it works out for you! ^.^

4.90 -> 4.94.X

Thank you very much!!!

the EXIM's version is 4.94.2, should be vulnerable. and i am sure TLS is also enabled. i can connected to the SMTP port (587) by socket and enter TLS tunnel by sending a 'STARTTLS' command. the response it gives me are all expected. However, when i try follow the tutorial and send a

"RCPT TO <postmaster> \r\n" command , it is failed as AUTH is required, which is not mentioned by the tutorial. in this case, should i consider the server is not vulnerable or how can i enter my credentials to login? if i need to login, do i login to the sending email account or the server?