How I Received 3 CVEs in Quick Heal Total Security

October 20, 2020 Ashutosh Barot

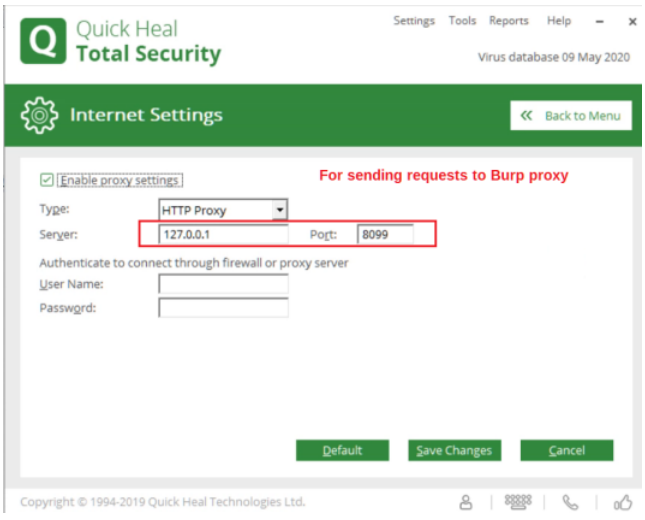
I was scrolling through Twitter and I thought I should be spending more time on testing thick clients. I decided to find vulnerabilities in an anti virus software as I like to hunt for bugs in cyber security products. I have used QuickHeal during my childhood days also they are doing great research in order to safeguard Indian cyber space.

In 2008, Pen Drives were a new thing in my small city, we were used to transfer games, movies, software setup files etc. using pendrives. This resulted in easy transmission of viruses, so I used to create QuickHeal Emergency CDs and help my friends with their infected machines.

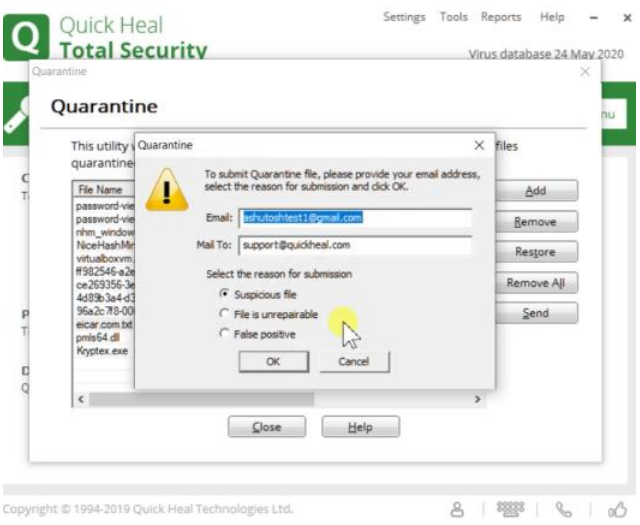
The target was finalised, QuickHeal total security 18.0, I purchased the premium version and started exploring its features. I ended up finding Three Medium risk vulnerabilities and rewarded for all of them, I have applied for Three CVE IDs for them. I am writing this article, which will be referred for the CVE IDs.

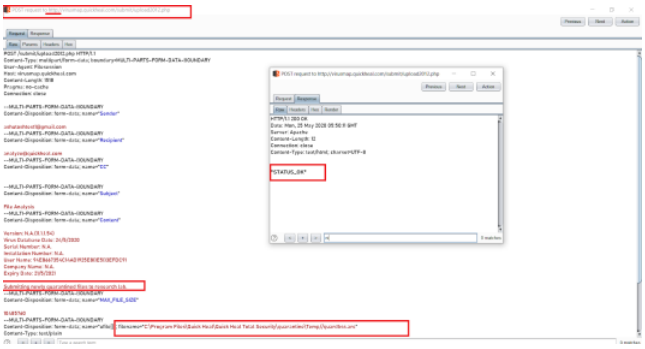
1. **Cleartext Transmission of Sensitive Information – CWE 319** [CVE-2020-27586]

I found that there is a proxy option in the software, and intercepted requests to Burpsuite.



The software had an option to send quarantined files to QH for further analysis. One other functionality to submit sysinfo file also used the same mechanism. This information was transmitted in clear text.





In order to exploit this issue, an attacker has to perform MITM attack first to intercept the communication.

CVE-2020-27586 has been assigned to this vulnerability by Mitre

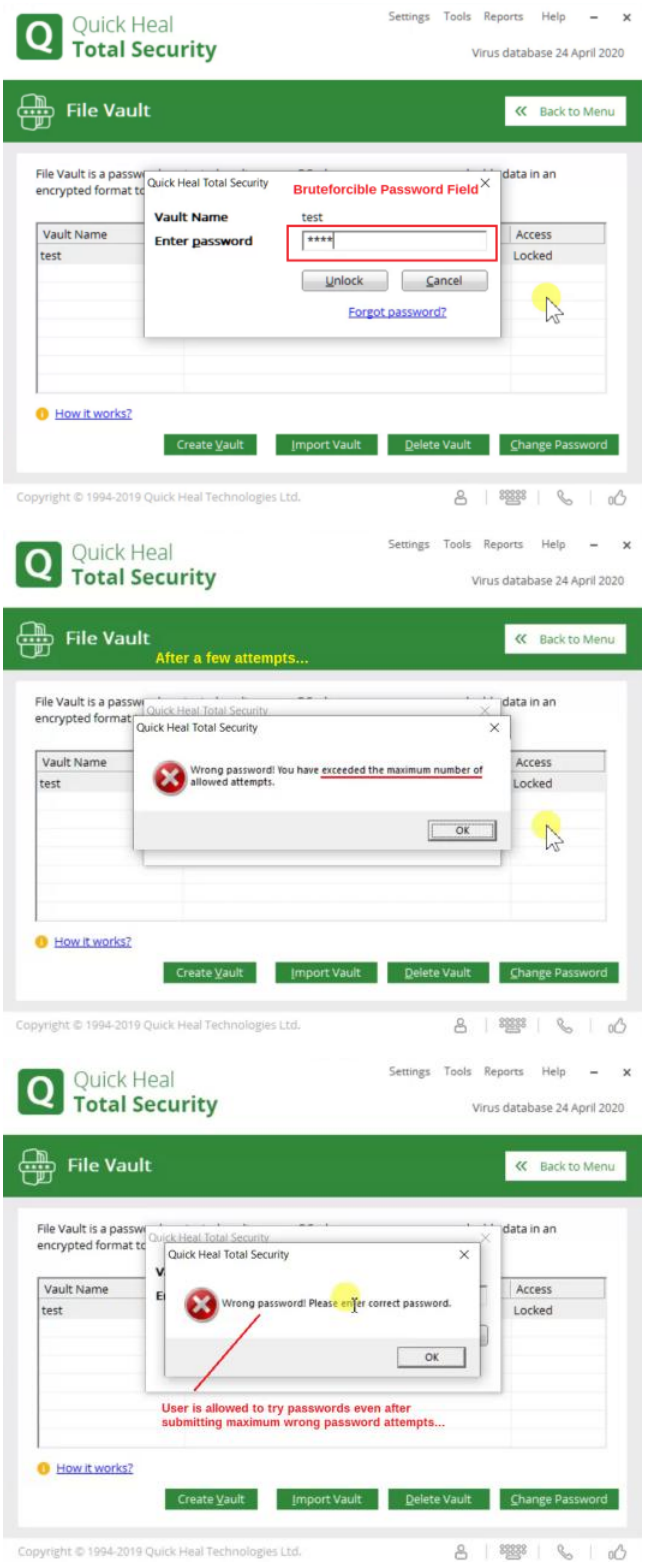
CVE
@CVEnew · **Follow**

CVE-2020-27586 Quick Heal Total Security before version 19.0 transmits quarantine and sysinfo files via clear

2. File Vault – Brute Forcible Password Field [CVE-2020-27587]

One interesting feature was 'File Vault'

File Vault is a feature of QuickHeal Total Security that allows users to store their files safely in a password protected 'vault'. But the field which accepts passwords was vulnerable to brute force attacks.



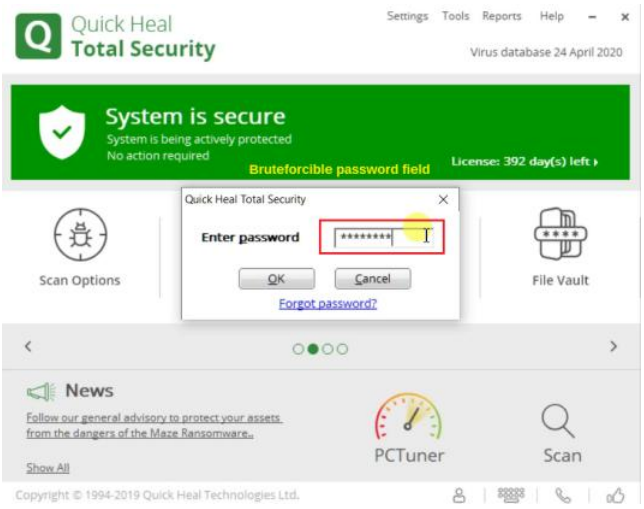
Local admin rights are required to access this functionality.

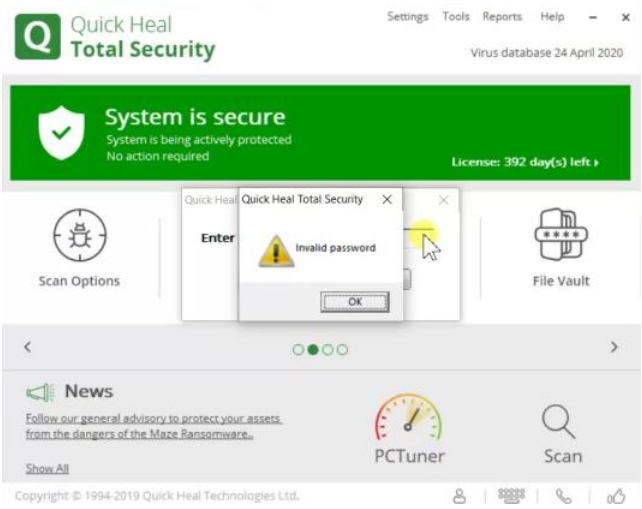
CVE
@CVEnew · **Follow**

CVE-2020-27587 Quick Heal Total Security before 19.0 allows attackers with local admin rights to obtain access to files in the File Vault via a

3. Brute Forcible Password Field – Settings [CVE-2020-27585]

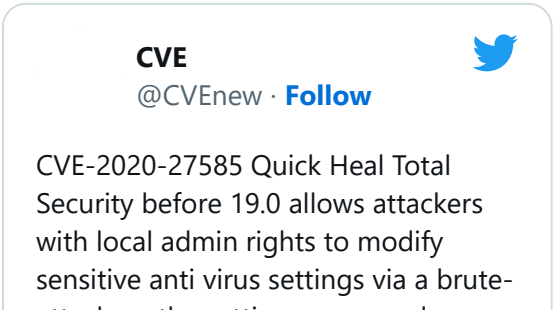
Same as the previous one, but this password field did not have any restriction for wrong password attempts.

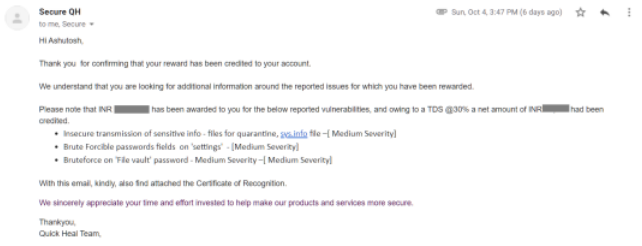




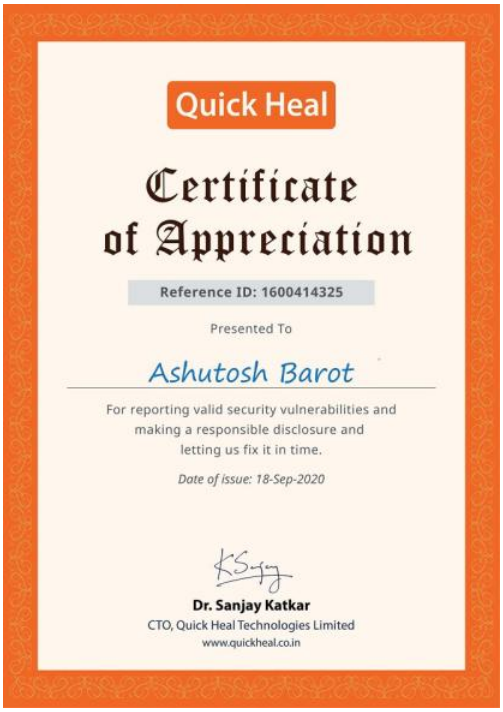
Impact of this issue was that an attacker could change settings of QHTS including disabling DNA scan, Disable anti keylogger, disable automatic updates, etc. Local admin rights are required to access this functionality.

CVE-2020-27585 has been assigned to this finding.





Quick Heal fixed these issues promptly in QuickHeal Total Security v19.0, and rewarded me for reporting these issues as per their responsible disclosure policy. Also received a certificate from Quick Heal's CTO Dr. Sanjay Katkar.



Ashutosh Barot

Ashutosh has found security issues that prevented leak of personal information belonging to 100 million+ people. He specialize in finding vulnerabilities in Web, Mobile applications, IT infrastructure, and consulting organizations on why, how, and when to fix them.

He is working with Deloitte since Jun 2017 as a Cyber Security Consultant/Engineer, Acknowledged by organizations like Google, Twitter, US Department of Defense, Symantec, United Nations, Rapid7, Trend Micro, Avira, United Airlines, IBM, Go Airlines, etc. for finding out security flaws in web applications.

ashutoshbarot.com

« Protect Your MongoDB – Story of "The Same Database"

How to Remove Cache, Local Data of a specific Website from Google Chrome? »

Recent Tweets