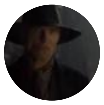


Furkan Göksel Follow

Jun 20 · 3 min read · Listen

Save

Comodo Antivirus Local Privilege Escalation Through Insecure File Move (CVE-2022–34008)

Introduction

> Comodo Antivirus has a quarantine flaw that allows privilege escalation. Exploitation uses an NTFS directory junction to restore a malicious DLL from quarantine into the System32 folder. By overwriting/putting a DLL which is used by a SYSTEM level process, one can elevate his/her privileges.
>
> I'm disclosing this vulnerability after waiting them for 60 days. They didn't respond my emails.

Description of the Vulnerability

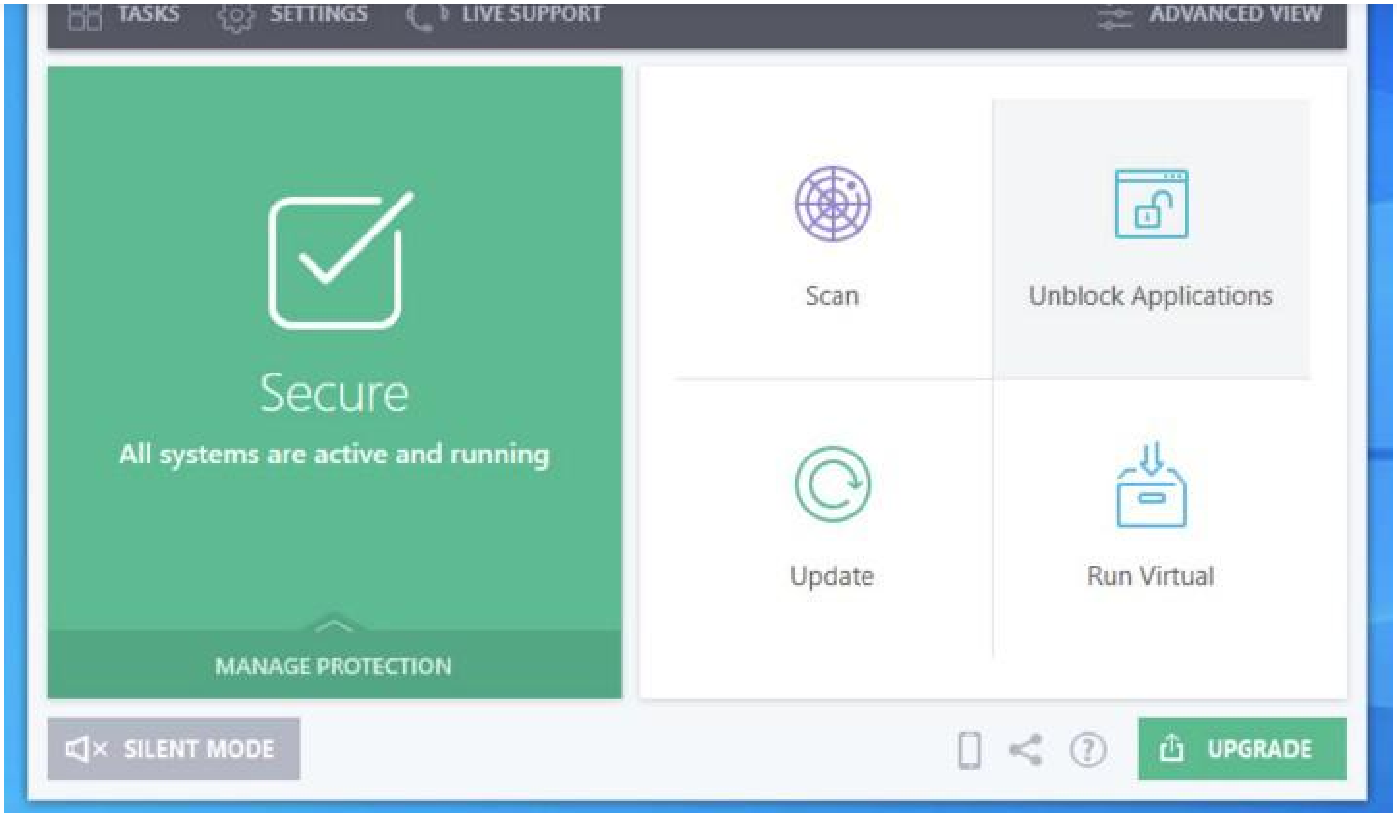
1. Title: Comodo Antivirus Local Privilege Escalation Through Insecure File Move

2. Product: Comodo Antivirus

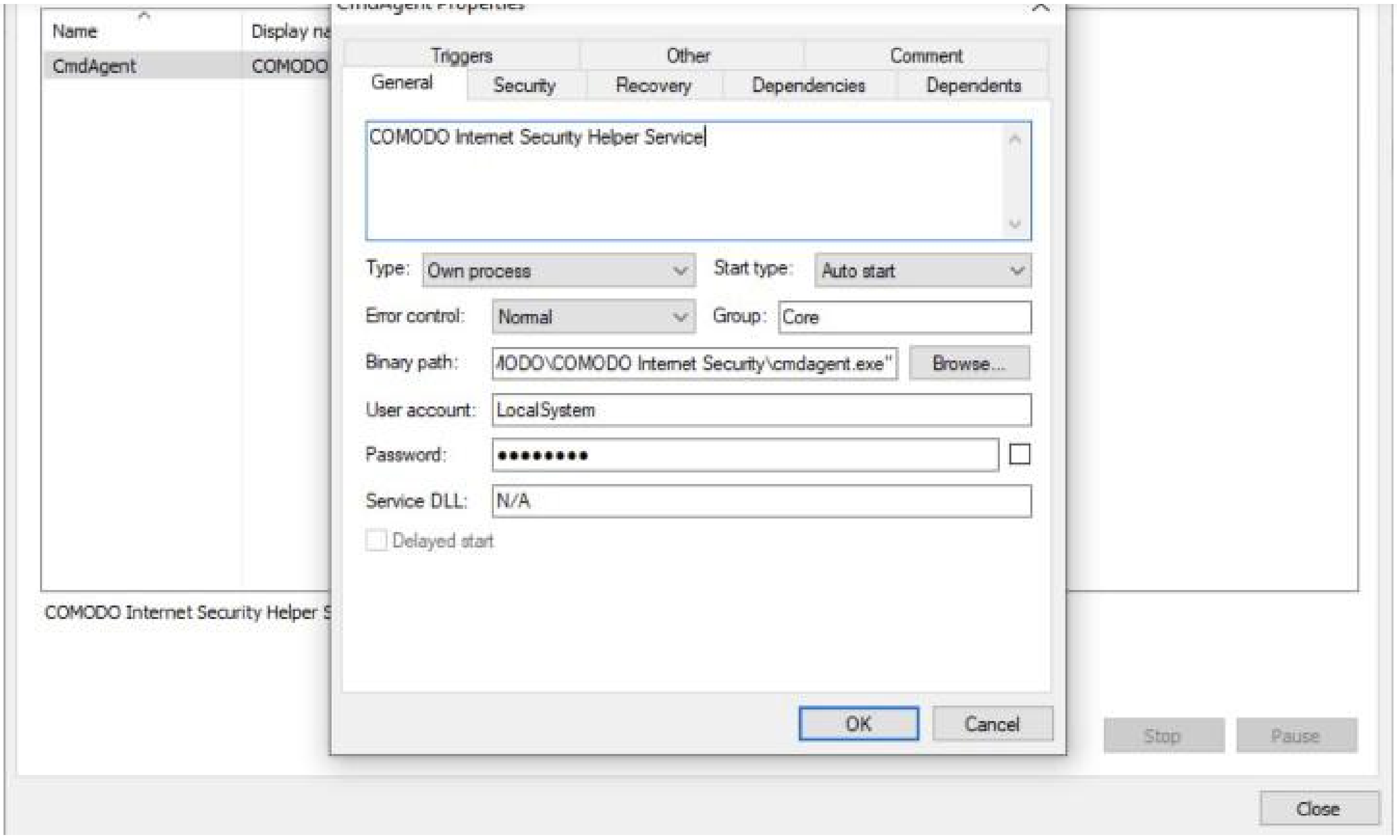
3. Version: 12.2.2.8012 (Latest Version on June 2022)

4. Homepage: https://antivirus.comodo.com/

5. Test Platform: Windows 10 19044



Comodo Antivirus has a service called **"Comodo Internet Security Helper Service"** which runs as the **SYSTEM.**



CmdAgent Properties

Name	Display na
CmdAgent	COMODO

Triggers | Other | Comment
General | Security | Recovery | Dependencies | Dependents

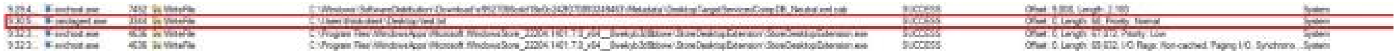
COMODO Internet Security Helper Service

Type: Own process
Start type: Auto start
Error control: Normal
Group: Core
Binary path: ΛODO\COMODO Internet Security\cmdagent.exe"
User account: LocalSystem
Password: ••••••••• □
Service DLL: N/A
□ Delayed start

COMODO Internet Security Helper S

One of the jobs that this service does is the quarantine feature.

When a malicious file is detected, it is first quarantined by the application with the default settings. In order to restore this malicious file, the user can unblock it from the unblock applications tab. While restoring the file, **the file is moved to its older location via SYSTEM privileges by the cmdagent.exe which is the process of that service.** For example, an EICAR file (test.txt in the screenshot) was moved to its original location by this process.



```
9:29:4... svchost.exe   7452 WriteFile C:\Windows\SoftwareDistribution\Download\[illegible]\Metadata\Desktop\TargetServices\Comp.DB_Neutral.xml.cab  SUCCESS  Offset: 9,808, Length: 2,160  System
9:30:5... cmdagent.exe  3444 WriteFile C:\Users\[illegible]\Desktop\test.txt  SUCCESS  Offset: 0, Length: 68, Priority: Normal  System
9:32:3... svchost.exe   4636 WriteFile C:\Program Files\WindowsApps\Microsoft.WindowsStore_22204.1401.7.0_x64__8wekyb3d8bbwe\StoreDesktopExtension\StoreDesktopExtension.exe  SUCCESS  Offset: 0, Length: 61,312, Priority: Low  System
9:32:3... svchost.exe   4636 WriteFile C:\Program Files\WindowsApps\Microsoft.WindowsStore_22204.1401.7.0_x64__8wekyb3d8bbwe\StoreDesktopExtension\StoreDesktopExtension.exe  SUCCESS  Offset: 0, Length: 69,632, I/O Flags: Non-cached, Paging I/O, Synchrono...System
```

Because of this, a non-admin user can put any file he/she wants to privileged locations like System32 by abusing the NTFS junctions. After that, he/she can use this ability to escalate his/her privileges to SYSTEM by overwriting/putting malicious DLLs under the System32 folder to abuse DLL Search Order.

content to this file to trigger the quarantine feature. After that, Comodo Antivirus detects this file and quarantines it.

When the file is in the quarantine, we can create an NTFS junction by using the CreateMountPoint tool from our symbolic link toolkit. **We can arrange this NTFS junction so that it redirects any write operation for the directory on the Desktop to the System32 directory.** When the NTFS junction is ready, if we restore the file, we can realize that it is now placed under the System32 directory.

I showed these steps in a Youtube video. You can watch it below. To escalate privilege, you can overwrite or put a malicious DLL, whose name is the same as a DLL imported by a SERVICE level process, under the System32 folder.