

[Open in app](#)[Get started](#)

Furkan Göksel

[Follow](#)

Jun 14 · 2 min read · [Listen](#)



Save



Adaware Protect Local Privilege Escalation through Insecure Service Permissions (CVE-2022-31464)

Introduction

*Adaware Protect has a service called Adaware Protect Service which runs as the Local System Account. Since **Everyone** has **Full Control** over this service, a low privilege user can escalate his/her privileges to the **SYSTEM** level.*

I'm disclosing this vulnerability after waiting them for 60 days.

Description of the Vulnerability

1. Title: Adaware Protect Local Privilege Escalation through Insecure Service Permissions
2. Product: Adaware Protect
3. Version: 1.2.495.4325 (Latest Version on 14 June 2022)
4. Homepage: <https://www.adaware.com>
5. Test Platform: Windows 10 19044

During the installation of Adaware Antivirus, you can also install Adaware Protect as you can see from the screenshot below.





Open in app

Get started

GET IT FREE!

Add your extra layer of security & privacy with
AdawareProtect

ONLINE PROTECTION:
Block malicious websites that contain malware and phishing scams.

SAFE BROWSER:
Browse the web securely and ad free.

PRIVATE SEARCH:
Go beyond Incognito mode. Protect your browsing history from being tracked.

MICROPHONE & CAMERA BLOCKER:
Worried you're being seen or heard? Use our free mic & cam blockers.

ADD FOR FREE

NO THANKS

By installing this software, you accept our [License Agreement](#) & [Privacy Policy](#)

We use cookies to customize content and to analyze our traffic. We also share information about your use of our site with our partners according to our Privacy policy. You can manage your preferences in Google's Performance of services.

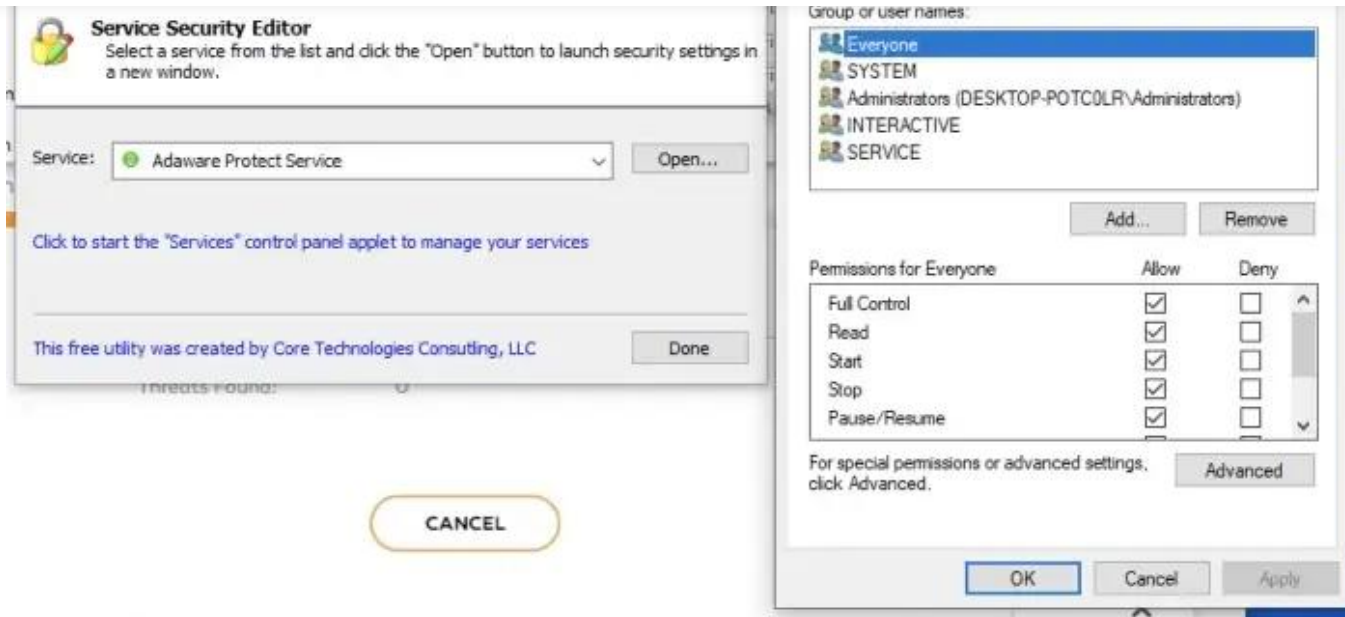
X

After the installation, I realized that a new service is created whose name is Adaware Protect Service which executes AdawareProtectService.exe, and the process which is created by this service is running as SYSTEM privileges which is the highest privilege on Windows Systems.

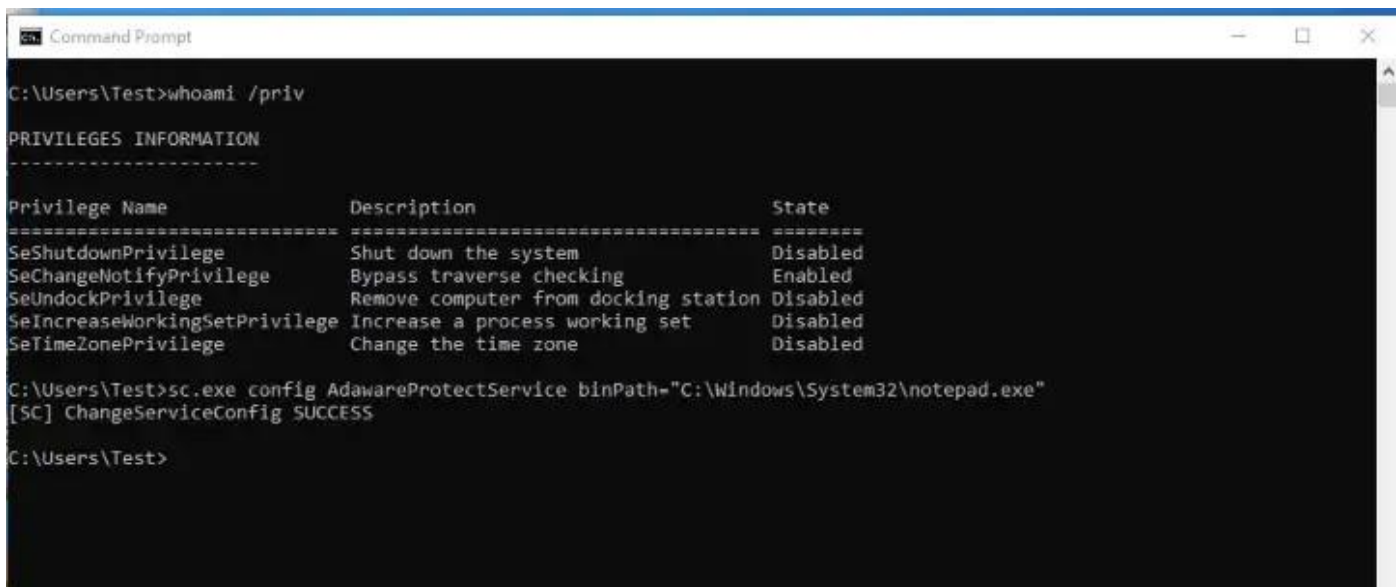
Process	PID	Private Bytes	Working Set	Private Bytes	Working Set	Process Name	Service Name	Image Path	Session
AdAwareService.exe	12812	2.41	2.74 MB/s	24.79 MB	NT AUTHORITY\SYSTEM	adaware service	System	0	0
AdawareProtectService.exe	13588	5.32	274.58 kB...	9.73 MB	NT AUTHORITY\SYSTEM	Adaware Protect	System	0	0

I checked the permissions for this service and saw that EVERYONE has full control of that service configuration which may lead to escalate privileges from low privileged to SYSTEM level privilege.



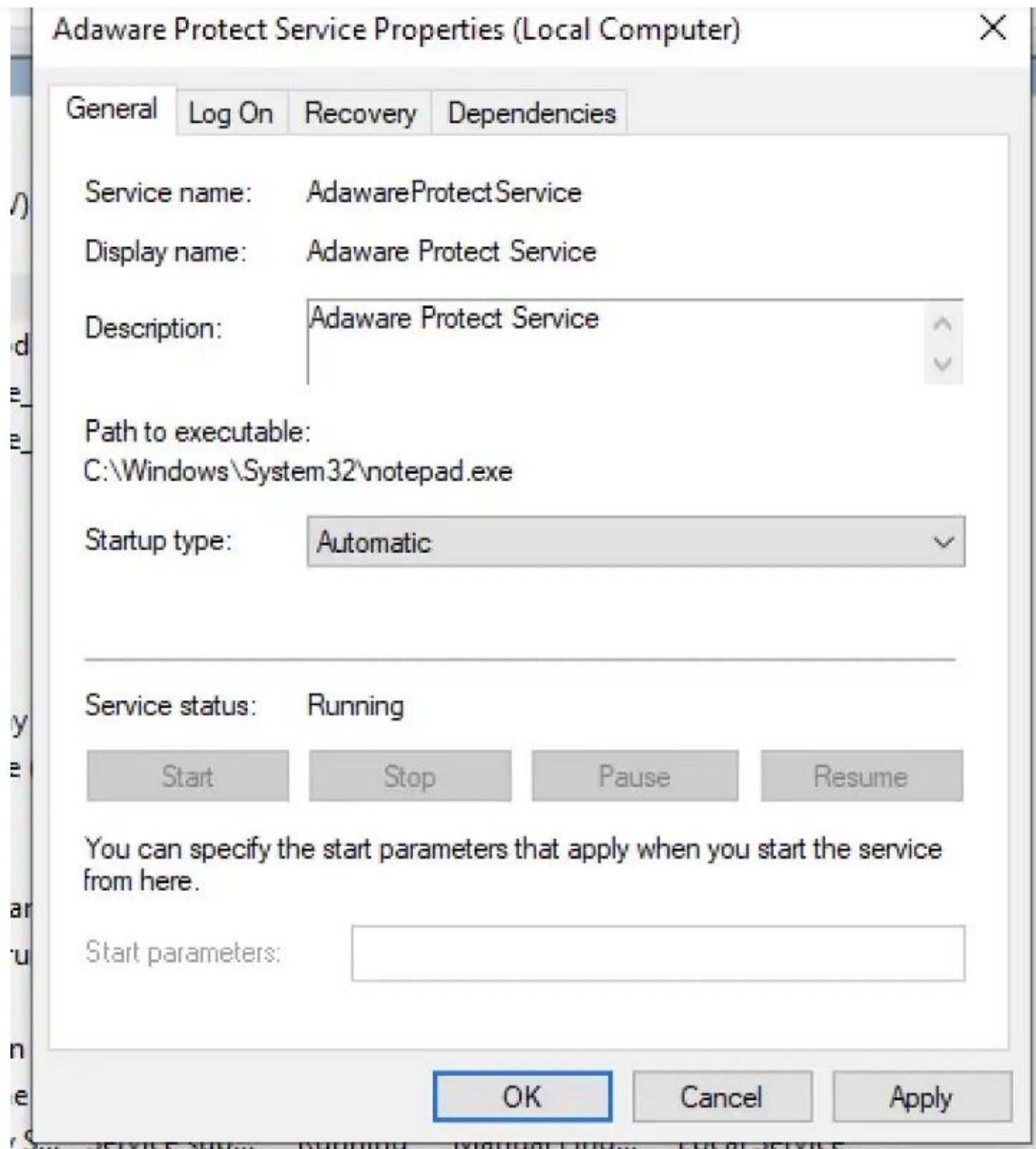
[Open in app](#)[Get started](#)

From a low privileged account, you can change the service binary path to any binary that you want. In this way, you can execute this binary as the SYSTEM.



You can also confirm this change from the Services GUI.



[Open in app](#)[Get started](#)

After changing its startup type to Disable and rebooting the computer (because you cannot stop the service directly), you can see that your selected binary is executed as SYSTEM (in our case it's notepad.exe).





Open in app

Get started

By following the same steps, anyone can take any permissions that he/she wants over an executable from a low privilege account.

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app





Open in app

Get started

