ZeroTierOne for windows local privilege escalation because of incorrect directory privilege in zerotier/zerotierone

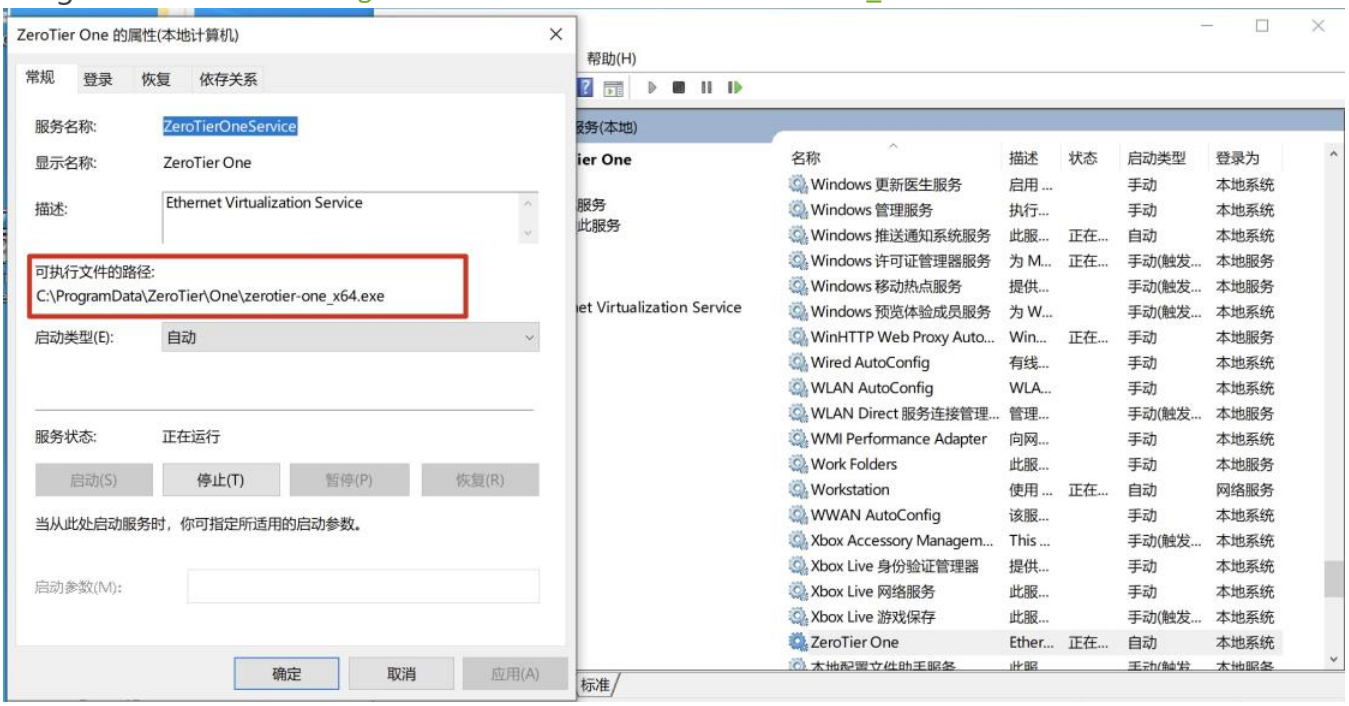
Valid Reported on Apr 9th 2022

Description

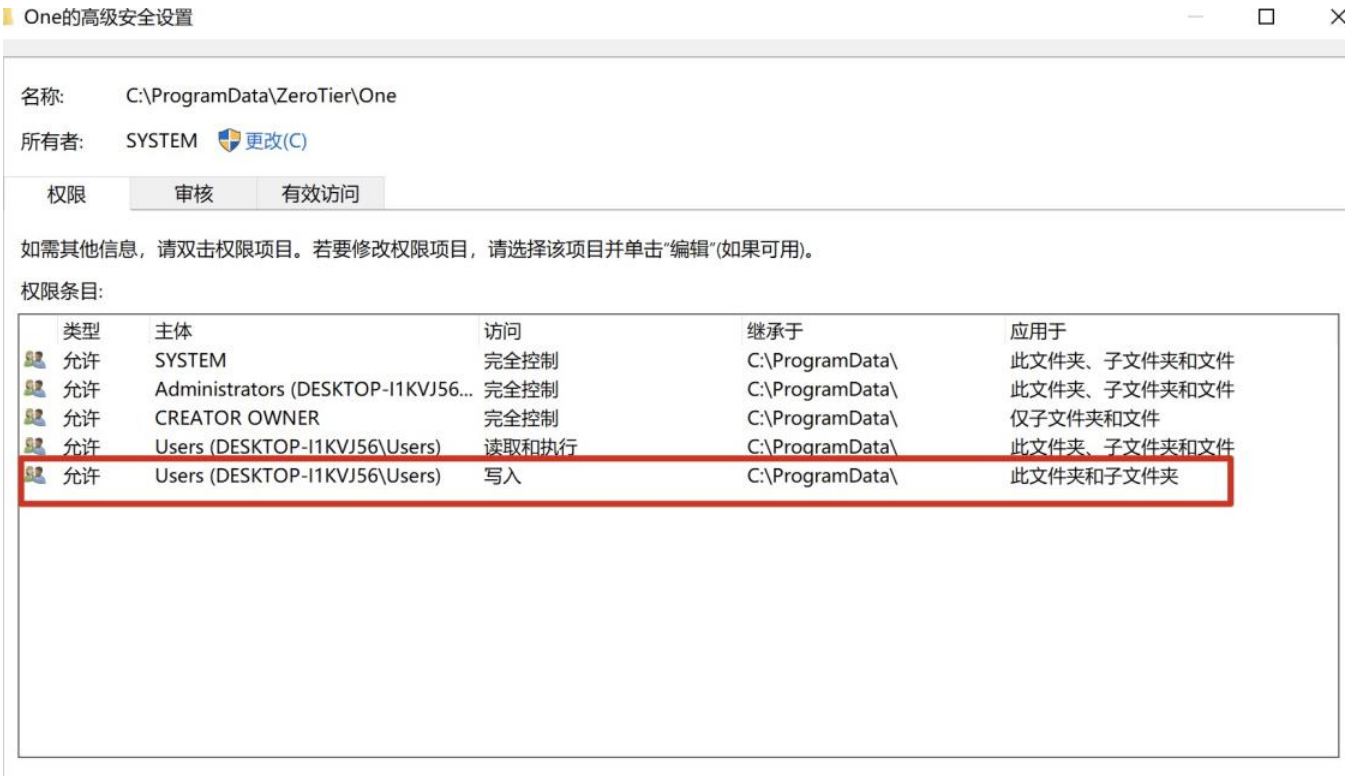
When administrators install zerotierone for windows, it will install ZeroTierOneService, the ImagePath of it is `C:\ProgramData\ZeroTier\One\zerotier-one_x64.exe` , however, the permission of `C:\ProgramData\ZeroTier\One\` is incorrect, an attacker with low privilege can get system privilege by this vuln.

Proof of Concept

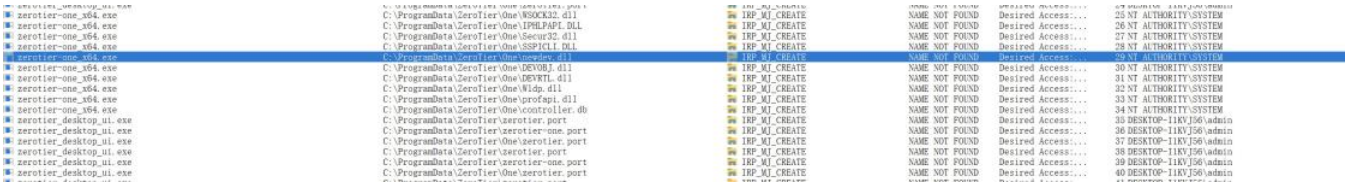
When administrators install zerotierone for windows, it will install ZeroTierOneService, the ImagePath of it is `C:\ProgramData\ZeroTier\One\zerotier-one_x64.exe` .



However,the permission of `C:\ProgramData\ZeroTier\One\` is incorrect, all Users have write permission of `C:\ProgramData\ZeroTier\One` and its subdirectories.



When ZeroTierOneService starts, it will try to load some dlls under `C:\ProgramData\ZeroTier\One` .



So an attacker with low privilege can exploit it and gain a system privilege by dll hijacking because of ZeroTierOneService running as SYSTEM.

Impact

Local Privilege Escalation

CVE
CVE-2022-1316
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
High (8.8)

Registry
Other

Affected Version

1.8.7 and before

Visibility
Public

Status
Fixed

Found by

ycdxsb
@ycdxsb
amateur

This report was seen 822 times.

We are processing your report and will contact the **zerotier/zerotierone** team within 24 hours. 8 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 8 months ago

We have contacted a member of the **zerotier/zerotierone** team and are waiting to hear back 8 months ago

Sean OMeara 7 months ago Maintainer

Hello! We have shipped a fix for this in 1.8.8 and will be releasing a blog post about it shortly.

Sean OMeara 7 months ago Maintainer

Is there a time frame for disclosure and CVE publication?

Sean OMeara validated this vulnerability 7 months ago

ycdxsb has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Sean OMeara marked this as fixed in 1.8.8 with commit ffb444 7 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sean OMeara 7 months ago Maintainer

Just wanted to drop a note saying "thank you" for the report. This is a really cool platform. Cheers!

Sean OMeara 7 months ago Maintainer

https://www.zerotier.com/2022/04/11/zerotier-for-windows-local-privilege-escalation/

Jamie Slome 7 months ago Admin

@Sean - thanks for the work here! Happy to hear you had a positive experience on the platform. We are releasing some updates today to the platform which will give the maintainer and researcher better insight into the CVE status of the report :)

Sign in to join this conversation

FAQ

contact us

terms

privacy policy

Chat with us