CVE-2021-35508: Privilege Escalation via Weak Windows Service Permissions

Christina Marshall, MBA
Third Party Risk Analyst at Trinity Health (HQ Michigan)
Published Aug 27, 2021

August 27, 2021|Christina Marshall, MBA

In this post I will detail a recent privilege escalation via weak Windows service permissions vulnerability I discovered while preforming a security test of TeraRecon AQNetClient.

DESCRIPTION

Privilege escalation via weak Windows service permissions is something that can be exploited relatively easy and with various tools and methods.

Windows services are applications that run hidden in the background and automatically start when the computer boots, can be paused and restarted, and do not show any user interface.

Often, Windows environments are discovered with services that run with SYSTEM privileges and do not have the appropriate permissions set by the administrator. The SYSTEM account is the highest privilege level in the Windows user model.

Services created by SYSTEM having weak permissions can lead to privilege escalation. For example, if a low privileged user can modify the service configuration, i.e., change the binPath to a malicious binary and restart the service then, the malicious binary will be executed with SYSTEM privileges.

ATTACK SCENARIO

- A low privileged user can change service configuration, for example, change the service binary that the service launches when it starts.
- A low privileged user can overwrite the binary that the service launches when it starts.

AFFECTED SOFTWARE

TeraRecon AQNetClient version 4.4.13

EXPLOIT WALKTHROUGH

access.

In addition, the following BAT file was found within the directory: C:\AQNetClient

From here we can modify the service (NMSAccess32.exe) and point its binary to our malicious binary.

Step 1: Copy calc.exe to directory C:\AQNetClient

NOTE: calc.exe is a binary used to demonstrate this POC, but any malicious payload can be used to replace calc.exe

Step 2: Rename calc.exe as NMSAccess32.exe

Step 3: Open Task Manager

Step 4: Open Services and start NMSAccess

Step 4: View NMSAccess32.exe in Task Manager

Step 5: Note NMSAccess32.exe is running as user: SYSTEM

THE PATCH

TeraRecon patched this bug in the 4.4.14P1, minor patch release. The purpose of this release is to provide corrections to software deficiencies including the Thin Client security vulnerability of the NMSAccess service. According to TeraRecon, this patch release must be installed after upgrading the software to the 4.4.14 version. TeraRecon also mentions a manual correction is available instead of the patch within their *Release Notes for Customer Use*.

CONCLUSION

As noted, a lot of applications have weak Windows service permissions vulnerabilities. In the case of TeraRecon AQNetClient, there is a patch or a manual correction to mitigate this vulnerability, but not all applications can be patched. In these cases, Microsoft has detailed some best practices when creating Windows services (see Descriptions of some best practices when you create Windows Services (microsoft.com)).

REFERENCES

https://terarecon.sharefile.com/share/view/s05c8b7792f354a2d8115789a02449c4a

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35508

https://support.microsoft.com/en-us/topic/descriptions-of-some-best-practices-when-you-create-windows-services-13ca508e-231d-43e6-b960-3b04ccf79064

uCertify CySA+ Test Prep
Feb 9, 2019

Others also viewed

LOLBin Attacks With Scheduled Tasks (T1053.005) and How To Detect Them
Julian-Ferdinand Vögele · 10mo

Explore topics

Workplace
Job Search
Careers
Interviewing
Salary and Compensation
Internships
Employee Benefits
See All