Advisory: Total Commander 9.51 Privilege Escalation (CVE-2020-17381)

Summary

Product: Total Commander
Affected version: 9.51
Vendor: Ghisler Software GmbH
Fixed Version: Won't fix
Tested Versions:

- Total Commander v.9.51 32-bit
- Total Commander v.9.51 64-bit
- Total Commander v.9.51 32-bit + 64-bit combined

CVE Reference: CVE-2020-17381
CWE Reference: CWE-276

Problem Description

The folder permissions on the default installation directory `%SYSTEMDRIVE%\totalcmd\` allow anyone in the "Authenticated Users" group to modify its contents. To exploit this vulnerability, a local attacker can replace the `TOTALCMD64.EXE` with a crafted binary with the same name. Afterwards, if another user starts the executable, the attacker's code will be executed in the context of the user who started it.

Impact

By replacing the binary an attacker can execute code, allowing potential privilege escalation and lateral movement.

Workaround

It is advised to change the installation directory to `%SYSTEMDRIVE%\Program Files\` or `%SYSTEMDRIVE%\Program Files(x86)\` . By default, these directories allow "Authenticated Users" to only read and execute the directory contents.

Notes

The issue was reported to the vendor, who decided not to fix the issue.

Proof Of Concept

Proof of Concept on Vimeo

Steps in the video:

1. Download and install Total Commander with default settings as administrator.
2. Attacker starts netcat listener.
3. User (attacker) logs in and replaces the `TOTALCMD64.EXE` with a malicious binary.
4. Administrator executes the malicious binary instead of Total Commander and a reverse shell with an administrator session spawns.

Disclosure Timeline

2020-07-22: Vulnerability discovered
2020-07-28: Vulnerability reported to vendor
2020-07-29: Vendor response
2020-07-30: Sent further explanation (PoC)
2020-07-30: Vendor states that a UAC bypass is needed to perform administrative tasks
2020-08-02: Further explanation of the attack vector and UAC
2020-08-03: Vendor decided they do not want to change so the current user base won't be affected, as most of them are local administrator anyway. Users that want additional security can choose to install the program in "Program Files"
2020-08-07: CVE reserved
2020-08-26: Informed vendor about publication
2020-08-27: Vendor agreed to the publication
2020-10-21: Published advisory

References

https://www.ghisler.com/download.htm
https://vimeo.com/442843440

EOF