

master



CVE_07_2019 / Report.pdf



GitHubAssessments Add files via upload

History

1 contributor

1.29 MB



Trezor Bridge - 2.0.27

(Windows)

August 09th, 2019.

Description:

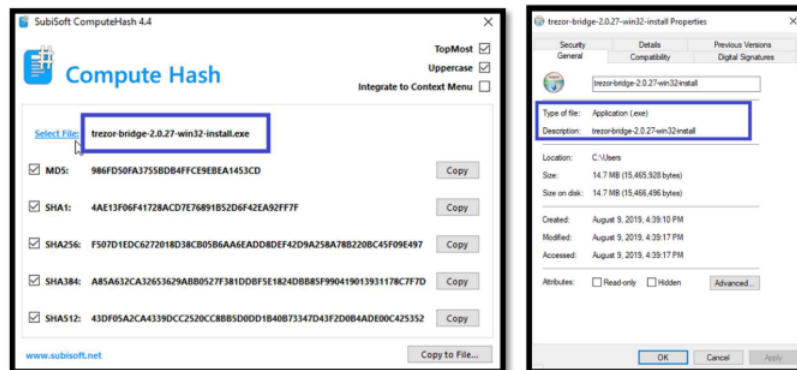
The Trezor wallet is used to secure digital assets (e.g. bitcoin and crypto currency). However, the Trezor Bridge application (i.e. Windows version) used to connect the hardware device and the internet browser was considered vulnerable in the aspect of privilege escalation. This vulnerability is related to functions such as SeDebugPrivilege and SeLoadPrivilege enabled by the application. For instance, an offensive package (i.e. mimikatz) is able to identify the presence of this type of privilege.

Attack Method: Malware could perform code injection in the process used by the Trezor Bridge application.

Exploit reference: at the www.exploit-db.com there is a reference to "Abusing Token Privileges For LPE".

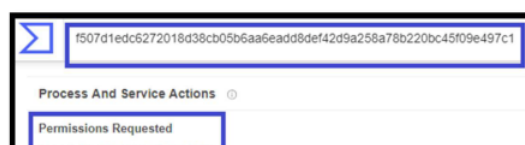
General mitigation strategy: limit the access of debug privileges to specific programs and users through group policy.

File identification



1

Permissions requested



Definition of permissions

docs.microsoft.com/en-us/windows/win32/secauthz/privilege-constants

Filter by title	SE_DEBUG_NAME TEXT("SeDebugPrivilege")	Required to debug and adjust the memory of a process owned by another account. User Right: Debug programs.
Authorization	SE_DELEGATE_SESSION_USER_IMPERSONATE_NAME TEXT("SeDelegateSessionUserImpersonatePrivilege")	Required to obtain an impersonation token for another user in the same session. User Right: Impersonate other users.
> About Authorization	SE_ENABLE_DELEGATION_NAME TEXT("SeEnableDelegationPrivilege")	Required to mark user and computer accounts as trusted for delegation. User Right: Enable computer and user accounts to be trusted for delegation.
> Using Authorization in C++	SE_IMPERSONATE_NAME TEXT("SeImpersonatePrivilege")	Required to impersonate. User Right: Impersonate a client after authentication.
> Using Authorization in Script	SE_INC_BASE_PRIORITY_NAME TEXT("SeIncreaseBasePriorityPrivilege")	Required to increase the base priority of a process. User Right: Increase scheduling priority.
> Using Authz API	SE_INCREASE_QUOTA_NAME TEXT("SeIncreaseQuotaPrivilege")	Required to increase the quota assigned to a process. User Right: Adjust memory quotas for a process.
Authorization Reference	SE_INC_WORKING_SET_NAME TEXT("SeIncreaseWorkingSetPrivilege")	Required to allocate more memory for applications that run in the context of users. User Right: Increase a process working set.
Authorization Constants	SE_LOAD_DRIVER_NAME TEXT("SeLoadDriverPrivilege")	Required to load or unload a device driver. User Right: Load and unload device drivers.
Authorization Constants	SE_LOCK_MEMORY_NAME TEXT("SeLockMemoryPrivilege")	Required to lock physical pages in memory. User Right: Lock pages in memory.
Account Rights Constants	SE_MACHINE_ACCOUNT_NAME TEXT("SeMachineAccountPrivilege")	Required to create a computer account. User Right: Add workstations to domain.
App Container SID Constants		
Auditing Constants		
Capability SID Constants		
Privilege Constants		
> Authorization Data Types		
> Authorization Enumerations		
> Authorization Functions		
> Authorization Interfaces		
> Authorization Objects		
> Authorization Structures		
> Microsoft.Interop.Security.AzRoles Assembly		

Exploit Reference

exploit-db.com/papers/42556

Much like SeRestorePrivilege, we can also take control of critical system files or folders to abuse DLL load order or other such techniques.

----- [3.1.9 **SeDebugPrivilege**

SeDebugPrivilege is very powerful, it allows the holder to debug another process, this includes reading and writing to that process' memory. This privilege has been widely abused for years by malware authors and exploit developers, and therefore many of the techniques that one would use to gain EoP through this privilege will be flagged by modern endpoint protection solutions.

There are a host of various memory injection strategies that can be used with this privilege that evade a majority of AV/HIPS solutions. Finding these is left as an exercise for the reader.