

Trezor Bridge - 2.0.27

(Windows)

August 09th, 2019.

Description:

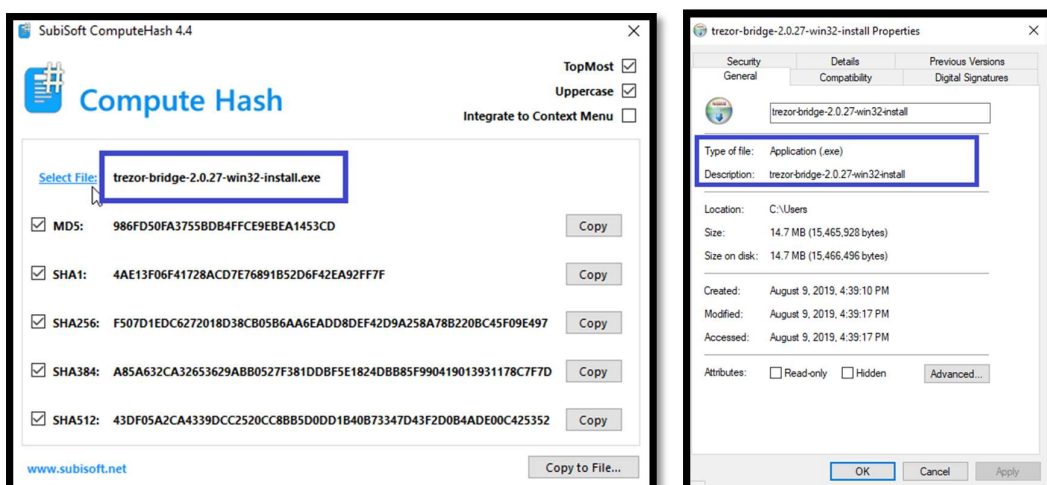
The Trezor wallet is used to secure digital assets (e.g. crypto currencies). However, the Trezor Bridge an application (i.e. Windows version) used to connect the hardware device and the internet browser was considered vulnerable in the aspect of privilege escalation. This vulnerability is related to 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.

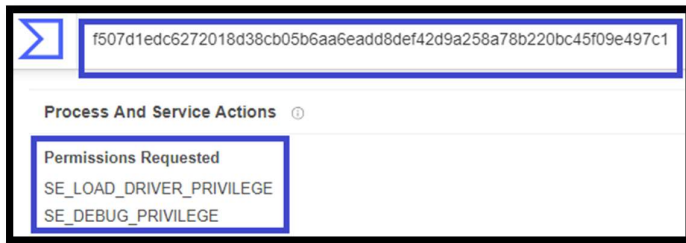
Exploit reference: at the www.exploit-db.com there is a reference to “Abusing Token Privileges For LPE”.

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

File identification



Permissions requested



Definition of permissions

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

Filter by title

Authorization

> About Authorization

> Using Authorization in C++

> Using Authorization in Script

> Using Authz API

> Authorization Reference

Authorization Reference

> Authorization Constants

Authorization Constants

Account Rights Constants

App Container SID Constants

Auditing Constants

Capability SID Constants

Privilege Constants

> Authorization Data Types

> Authorization Enumerations

> Authorization Functions

> Authorization Interfaces

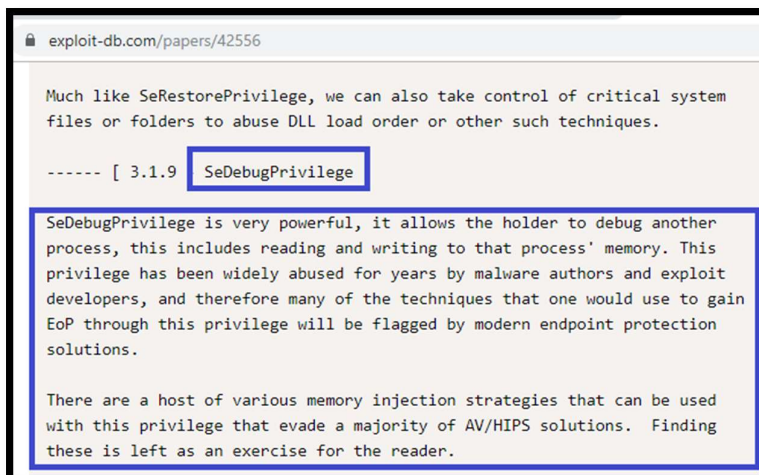
> Authorization Objects

> Authorization Structures

> Microsoft.Interop.Security.AzRoles Assembly

SE_DEBUG_NAME TEXT("SeDebugPrivilege")	Required to debug and adjust the memory of a process owned by another account. User Right: Debug programs.
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.
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.
SE_IMPERSONATE_NAME TEXT("SeImpersonatePrivilege")	Required to impersonate. User Right: Impersonate a client after authentication.
SE_INC_BASE_PRIORITY_NAME TEXT("SeIncreaseBasePriorityPrivilege")	Required to increase the base priority of a process. User Right: Increase scheduling priority.
SE_INCREASE_QUOTA_NAME TEXT("SeIncreaseQuotaPrivilege")	Required to increase the quota assigned to a process. User Right: Adjust memory quotas for a process.
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.
SE_LOAD_DRIVER_NAME TEXT("SeLoadDriverPrivilege")	Required to load or unload a device driver. User Right: Load and unload device drivers.
SE_LOCK_MEMORY_NAME TEXT("SeLockMemoryPrivilege")	Required to lock physical pages in memory. User Right: Lock pages in memory.
SE_MACHINE_ACCOUNT_NAME TEXT("SeMachineAccountPrivilege")	Required to create a computer account. User Right: Add workstations to domain.

Exploit Reference



----[2.2 - Relevant Exploitation Strategies

Previous, related work that provided influence and indirect guidance for this article's strategy is presented here. These related techniques are briefly detailed to provide background and to pay homage to those who came before us.

Cesar Cerrudos Easy Local Windows Kernel Exploitation paper released at Blackhat 2012 [1] introduced three different privilege escalation strategies, and pointed many exploit devs towards the power of abusing process tokens. The first technique demonstrated in the paper details the NULL ACL strategy, now partially mitigated, in which an arbitrary write could be leveraged to NULL a privileged object's ACL. This was and is a very common strategy for effectively migrating into more privileged processes.

The second Cerrudos strategy is a carpet bombing version of ours, in which an arbitrary write could enable all privileges in a process token. With these privileges enabled, one could exploit SeDebugPrivilege and migrate into a more privileged process, create tokens with SeCreateTokenPrivilege, or load kernel drivers with SeLoadDriverPrivilege.

Behavior Analysis and Techniques

MITRE ATT&CK™ Techniques Detection

MITRE ATT&CK™ Techniques Detection										
Minimal										
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Service Execution 1	Hooking 1	Hooking 1	Code Signing 1	Hooking 1	Application Window Discovery 1	Remote Desktop Protocol 1	Clipboard Data 1	Data Compromised 1	
		Kernel Modules and Extensions 1	Process Injection 2 1	File Deletion 1		File and Directory Discovery 1		Email Collection 1		
				Modify Registry 1 2 1		Peripheral Device Discovery 1 2				
				Process Injection 2 1		Query Registry 5 2				
						System Information Discovery 1				
						System Time Discovery 1				

trezor-bridge-2.0.27-win32-install.exe

This report is generated from a file or URL submitted to this webservice on August 9th 2019 19:51:28 (CEST)
Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.30 © Hybrid Analysis - [Learn more](#)

[Overview](#) | [Login to Download Sample \(15MiB\)](#) | [Downloads](#) | [External Reports](#)
[Re-analyze](#) | [Hash Not Seen Before](#) | [Show Similar Samples](#) | [Report Abuse](#)

malicious

Threat Score: 100/100
AV Detection: Marked as clean
Labeled as: Unavailable

[Link](#) | [Twitter](#) | [E-Mail](#)

Other Aspects

Interesting aspects that may require further review are the overlay (file-ratio), the raw size of the .bss section and the analysis of the Nullsoft Scriptable Install System (NSIS), which could be in some cases be related to dynamic link library attacks.

Sections					
Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	34188	34304	6.08	81ecd29fcd98071c91b59fbf637f22
.data	40960	224	512	1.59	8597f6ab584f83ce1f30bf6056109fbd
.rdata	45056	28356	28672	7.27	99e9ad8090242384592e7de6d7f8fd4d
.bss	73728	3917120	0	0	d41d8cd98f00b204e9800998ecf8427e
.idata	3993600	4760	5120	5.17	49e86989c0298358194be247cf3ed454
.ndata	4001792	540672	8192	0	0829f71740aab1ab98b33eae21dee122
.rsrc	4542464	16992	17408	5.89	42db1c3dc58baa99eabcdebe09036d05

References:

1. <https://wallet.trezor.io/#/bridge>
2. <https://trezor.io/>
3. <https://www.virustotal.com/gui/file/f507d1edc6272018d38cb05b6aa6eadd8def42d9a258a78b220bc45f09e497c1/behavior/Tencent%20HABO>
4. <https://www.hybrid-analysis.com/sample/f507d1edc6272018d38cb05b6aa6eadd8def42d9a258a78b220bc45f09e497c1>
5. <https://medium.com/palantir/windows-privilege-abuse-auditing-detection-and-defense-3078a403d74e>
6. <https://docs.microsoft.com/en-us/windows/win32/secauthz/privilege-constants>
7. <https://www.exploit-db.com/papers/42556>