Trezor Bridge - 2.0.27

(Windows)

August 09th, 2019.

Description:

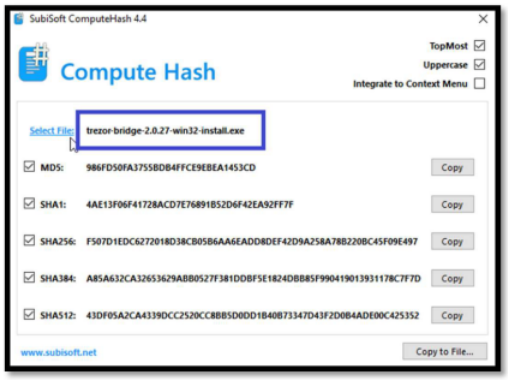
The Trezor wallet is used to secure digital assets (e.g. bitcoin and crypto currency). However, the Trezor Bridge an application (i.e. Windows version) used to connect the hardware device and the internet browser was considered vulnerable in the aspect of privilege escalation. This vulnerability is related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

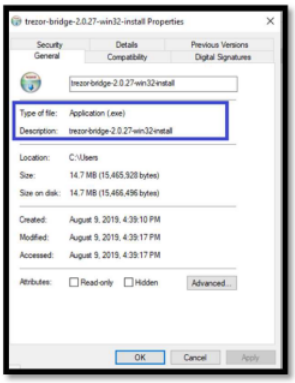
Attack Method: Malware could perform code injection in the process used by the Trezor Bridge application.

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.

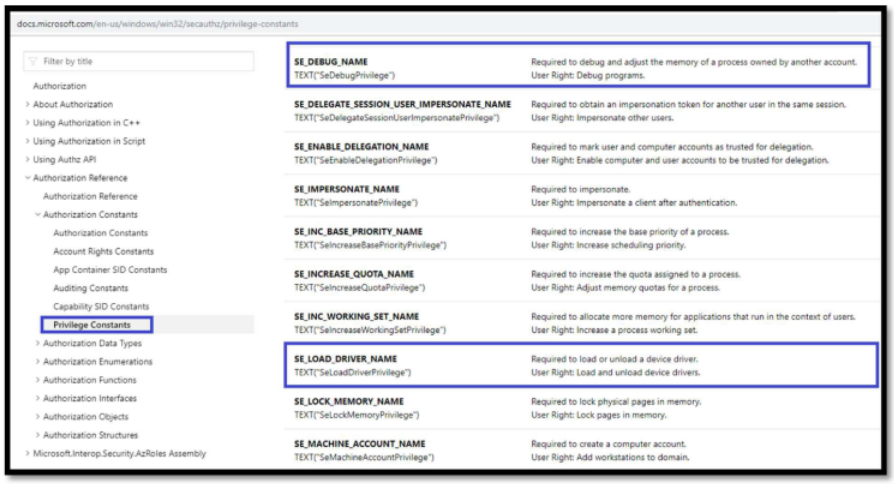
File identification





Permissions requested

Definition of permissions



Exploit Reference