Windows Sandbox: Analysis and Verification of Known Vulnerabilities

Ing. Jakub Štrom   Supervisor: Ing. Josef Kokeš, Ph.D.

Faculty of Information Technology, Czech Technical University in Prague

CTU CZECH TECHNICAL UNIVERSITY IN PRAGUE

Motivation

- Windows Sandbox is a built-in feature in Windows that provides an isolated environment
- Its implementation in the operating system spans multiple interesting components
- There were vulnerabilities in these components in the past
- The documentation of Windows Sandbox is lacking

Windows Sandbox

Windows Sandbox is built upon existing technology of Hyper-V and Windows Containers. It provides an easy way of creating isolated environment to the user. Figure 1 shows a high level representation of the Sandbox creation process including the components involved.

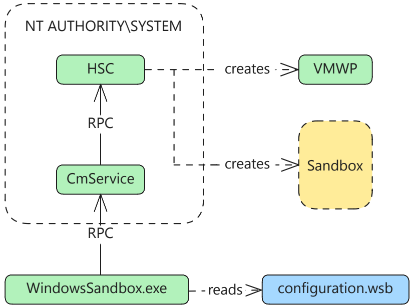

Figure 1. The creation of Windows Sandbox.

Although the created sandbox is ephemeral (state is preserved only during the session), it still needs a file system same as a regular Windows system. The file system of Windows Sandbox is shown in Figure 2.

Most of the required system files are shared with the base operating system. The files that cannot be shared are stored inside a so-called base layer. These base layer data are accessible from host operating system.

Vulnerabilities Analysis

Known vulnerabilities of relevant components that have been publicly disclosed by Microsoft were collected. These were analyzed using publicly available information and their issued patches. Described and verified whether the patch successfully addresses the issue for each vulnerability.

New vulnerability has been discovered in the cleanup logic of base layer files. Due to incorrect access control and following junction points, this could be abused by regular users to delete arbitrary files. Regular users could utilize this during an update of the Windows Sandbox to elevate to SYSTEM privileges.

Conclusion

- Improved the sparsely available information by providing a unified description of Windows Sandbox internals
- Both Windows 10 and Windows 11 implementations were described in detail, highlighting their differences
- Analyzed 10 known vulnerabilities in Windows Sandbox components
- Discovered and reported a new vulnerability CVE-2024-30076
- An Arbitrary File Deletion vulnerability which can be utilized to gain SYSTEM privileges under specific conditions
- Fixed in the 2024 June security update
- The new vulnerability has been identified based on previous vulnerability CVE-2023-36723

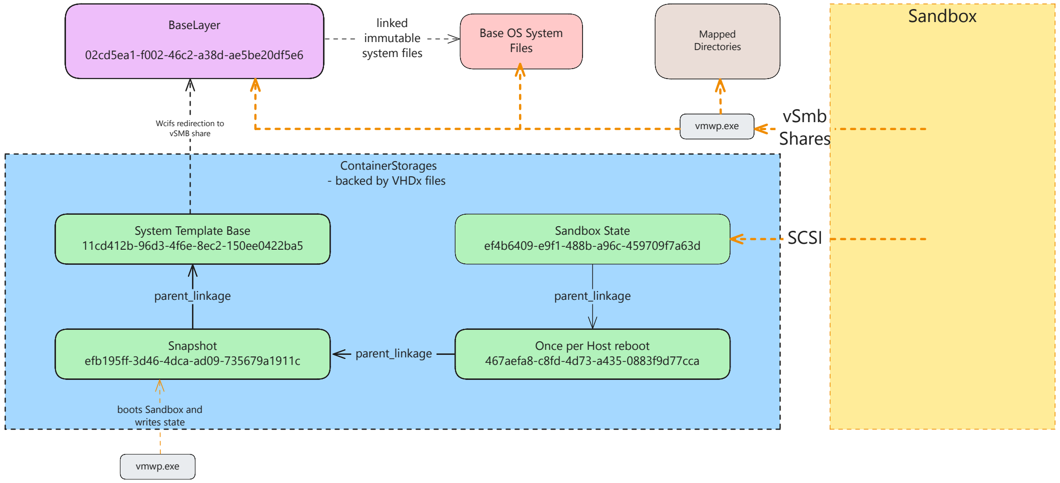
BaseLayer
02cd5ea1-f002-46c2-a38d-ae5be20df5e6
linked immutable system files
Base OS System Files
Mapped Directories
Sandbox
Wcifs redirection to vSMB share
vmwp.exe
vSmb Shares
ContainerStorages
- backed by VHDx files
System Template Base
11cd412b-96d3-4f6e-8ec2-150ee0422ba5
Sandbox State
ef4b6409-e9f1-488b-a96c-459709f7a63d
SCSI
parent_linkage
parent_linkage
Snapshot
efb195ff-3d46-4dca-ad09-735679a1911c
parent_linkage
Once per Host reboot
467aefa8-c8fd-4d73-a435-0883f9d77cca
boots Sandbox and writes state
vmwp.exe

Figure 2. Sandbox file system architecture.