NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise CMEP Practice Guide:

Assessment of SVCHOST.EXE

September 15, 2020

Background

In support of successful implementation of and compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards, the Electric Reliability Organization (ERO) Enterprise[1] adopted the Compliance Guidance Policy.[2] The Compliance Guidance Policy outlines the purpose, development, use, and maintenance of guidance for implementing Reliability Standards. According to the Compliance Guidance Policy, Compliance Guidance includes two types of guidance – Implementation Guidance and Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.[3]

Purpose

The purpose of this CMEP Practice Guide is to provide guidance to ERO Enterprise CMEP staff (CMEP staff) when assessing a Responsible Entity's process to enable only those logical network accessible ports (ports) that have been determined to be needed on applicable systems. This Practice Guide outlines aspects that CMEP staff should consider when testing and collecting evidence. This risk information can be used to inform CMEP staff's understanding of a Responsible Entity's security posture and commensurate Compliance Oversight (i.e., Compliance Oversight Plan, audit approach, etc.). CMEP Staff make compliance determinations in light of the facts and circumstances of individual Responsible Entities and the language of the Requirements.

Ports and Services

NERC Reliability Standard CIP-007-6 Requirement R1, Part 1.1 requires Responsible Entities to establish a process enabling only those ports on each applicable Cyber Asset needed for the function of the Cyber Asset.

When enabling (or allowing) ports, the Responsible Entity must provide evidence to demonstrate the need. Quality evidence shows not just the need, often referred to as a business reason, but also the details of how the entity reached its determination. Such decisions could establish the initial inputs to a Responsible Entity's configuration change management program, in compliance with CIP-010-2 Requirement R1, Part 1.1.4.

[1] The ERO Enterprise consists of NERC and the Regional Entities.

[2] The ERO Enterprise Compliance Guidance Policy is located on the NERC website at: https://www.nerc.com/pa/comp/guidance/Documents/Compliance%20Guidance%20Policy.pdf.

[3] Implementation Guidance provides a means for registered entities to develop examples or approaches to illustrate how registered entities could comply with a Standard that are vetted by industry and endorsed by the ERO Enterprise. CMEP Practice Guides differ from Implementation Guidance in that they address how ERO Enterprise CMEP staff executes compliance monitoring and enforcement activities, rather than examples of how to implement the Standard.

When a port is not needed, it must be disabled unless:

- There is a technical reason why it cannot be disabled, in which case a Technical Feasibility Exception (TFE) must be established and approved; or
- The device has no provision for disabling ports, in which case the entity must substantiate the device's inability to disable ports.

SVCHOST.EXE

Svchost.exe is a system process that can host from one to many Windows services in the Windows family of operating systems. Svchost.exe is essential in the implementation of shared service processes, where a number of services can share a process in order to reduce resource consumption.

Svchost.exe represents a challenge for a Responsible Entity to show compliance when services underlying SVCHost are not clearly identified. As a Windows Operating System (OS) process used to host other services, it does not open a port on its own behalf. Svchost.exe launches many commonly used services through Dynamic Linked Library files (e.g., Remote Procedure Calls, CryptSvc, EventLog, Schedule, etc.), which initiate logical network accessible ports. The hosted services listen on their own ports, but a simple process listing will show only svchost.exe as the process holding open the ports. These simple process listings do not adequately identify the actual service that is associated with the open port.

If CMEP staff samples a record that includes svchost.exe listed as a service for CIP-007-6 Requirement R1, Part 1.1, then CMEP staff should request further information regarding the actual service as launched by svchost.exe. With svchost.exe, the entity is required to know the enabled ports in conjunction with the specific service as described by the business need or justification.

Additionally, the language of the Standard states, "[…] including port ranges or services where needed to handle dynamic ports." The word "or" refers to instances where a dynamic service, such as svchost.exe, may not consistently open on a specific port. Typically, the port (or port range) and the service (not launchers like svchost.exe) should be known to establish need.

Conclusion

In assessing a Responsible Entity's ports and services controls, CMEP staff should consider processes that host other services (such as Svchost.exe) as one part of a Responsible Entity's evidence for CIP-007-6 Requirement R1, Part 1.1. Additional evidence would be required to demonstrate the Responsible Entity's determined need.