Network Allowlists, Mitigation M0807 - ICS

Archived: 2026-04-05 13:40:00 UTC

ICS T0800 Activate Firmware Update Mode

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0878 Alarm Suppression

Utilize network allowlists to restrict unnecessary connections to network devices (e.g., comm servers, serial to ethernet converters) and services, especially in cases when devices have limits on the number of simultaneous sessions they support.

ICS T0802 Automated Collection

Utilize network allowlists to restrict unnecessary connections to network devices (e.g., comm servers, serial to ethernet converters) and services, especially in cases when devices have limits on the number of simultaneous sessions they support.

ICS T0803 Block Command Message

Utilize network allowlists to restrict unnecessary connections to network devices (e.g., comm servers, serial to ethernet converters) and services, especially in cases when devices have limits on the number of simultaneous sessions they support.

ICS T0804 Block Reporting Message

Utilize network allowlists to restrict unnecessary connections to network devices (e.g., comm servers, serial to ethernet converters) and services, especially in cases when devices have limits on the number of simultaneous sessions they support.

ICS T0805 Block Serial COM

Implement network allowlists to minimize serial comm port access to only authorized hosts, such as comm servers and RTUs.

ICS T0806 Brute Force I/O

Utilize network allowlists to restrict unnecessary connections to network devices (e.g., comm servers, serial to ethernet converters) and services, especially in cases when devices have limits on the number of simultaneous sessions they support.

ICS T0858 Change Operating Mode

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0884 Connection Proxy

Network allowlists can be implemented through either host-based files or system host files to specify what external connections (e.g., IP address, MAC address, port, protocol) can be made from a device. Allowlist techniques that operate at the application layer (e.g., DNP3, Modbus, HTTP) are addressed in the Filter Network Traffic mitigation.

ICS T0879 Damage to Property

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0868 Detect Operating Mode

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0816 Device Restart/Shutdown

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0838 Modify Alarm Settings

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0839 Module Firmware

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0861 Point & Tag Identification

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0843 Program Download

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0845 Program Upload

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0886 Remote Services

Network allowlists can be implemented through either host-based files or system host files to specify what external connections (e.g., IP address, MAC address, port, protocol) can be made from a device.

ICS T0848 Rogue Master

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0856 Spoof Reporting Message

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0869 Standard Application Layer Protocol

Network allowlists can be implemented through either host-based files or system host files to specify what external connections (e.g., IP address, MAC address, port, protocol) can be made from a device. Allowlist techniques that operate at the application layer (e.g., DNP3, Modbus, HTTP) are addressed in the Filter Network Traffic mitigation.

ICS T0857 System Firmware

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

ICS T0855 Unauthorized Command Message

Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [1]

Source: https://attack.mitre.org/mitigations/M0807