Execution Prevention, Mitigation M1038 - Enterprise

Archived: 2026-04-05 16:22:53 UTC

Enterprise T1548 Abuse Elevation Control Mechanism

System settings can prevent applications from running that haven't been downloaded from legitimate repositories which may help mitigate some of these issues. Not allowing unsigned applications from being run may also mitigate some risk.

.004 Elevated Execution with Prompt

System settings can prevent applications from running that haven't been downloaded through the Apple Store which may help mitigate some of these issues. Not allowing unsigned applications from being run may also mitigate some risk.

Enterprise T1547 .004 Boot or Logon Autostart Execution: Winlogon Helper DLL

Identify and block potentially malicious software that may be executed through the Winlogon helper process by using application control [1] tools like AppLocker [2] [3] that are capable of auditing and/or blocking unknown DLLs.

.006 Boot or Logon Autostart Execution: Kernel Modules and Extensions

Application control and software restriction tools, such as SELinux, KSPP, grsecurity MODHARDEN, and Linux kernel tuning can aid in restricting kernel module loading.[4][5][6][7][8]

.009 Boot or Logon Autostart Execution: Shortcut Modification

Prevents malicious shortcuts or LNK files from executing unwanted code by ensuring only authorized applications and scripts are allowed to run.

Enterprise T1059 Command and Scripting Interpreter

Use application control where appropriate. For example, PowerShell Constrained Language mode can be used to restrict access to sensitive or otherwise dangerous language elements such as those used to execute arbitrary Windows APIs or files (e.g., `Add-Type`).[9]

.001 PowerShell

Use application control where appropriate. PowerShell Constrained Language mode can be used to restrict access to sensitive or otherwise dangerous language elements such as those used to execute arbitrary Windows APIs or files (e.g., `Add-Type`).[9]

.002 AppleScript

Use application control where appropriate.

.003 Windows Command Shell

Use application control where appropriate.

.004 Unix Shell

Use application control where appropriate. On ESXi hosts, the `execInstalledOnly` feature prevents binaries from being run unless they have been packaged and signed as part of a vSphere installation bundle (VIB).[10]

.005 Visual Basic

Use application control where appropriate. VBA macros obtained from the Internet, based on the file's Mark of the Web (MOTW) attribute, may be blocked from executing in Office applications (ex: Access, Excel, PowerPoint, Visio, and Word) by default starting in Windows Version 2203.[11]

.006 Python

Denylist Python where not required.

.007 JavaScript

Denylist scripting where appropriate.

.008 Network Device CLI

TACACS+ can keep control over which commands administrators are permitted to use through the configuration of authentication and command authorization. [12]

.009 Cloud API

Use application control where appropriate to block use of PowerShell CmdLets or other host based resources to access cloud API resources.

.010 AutoHotKey & AutoIT

Use application control to prevent execution of `AutoIt3.exe`, `AutoHotkey.exe`, and other related features that may not be required for a given system or network to prevent potential misuse by adversaries.

.011 Lua

Denylist Lua interpreters where appropriate.

.013 Container CLI/API

Deny scripting where appropriate. Tools such as Python or Go can utilize Kubernetes and Docker within a client library and execute commands within their application.

Enterprise T1609 Container Administration Command

Use read-only containers, read-only file systems, and minimal images when possible to prevent the execution of commands.[13] Where possible, also consider using application control and software restriction tools (such as those provided by SELinux) to restrict access to files, processes, and system calls in containers.[14]

Enterprise T1611 Escape to Host

Use read-only containers, read-only file systems, and minimal images when possible to prevent the running of commands.[13] Where possible, also consider using application control and software restriction tools (such as those provided by SELinux) to restrict access to files, processes, and system calls in containers.[14]

Enterprise T1546 .002 Event Triggered Execution: Screensaver

Block .scr files from being executed from non-standard locations.

.006 Event Triggered Execution: LC_LOAD_DYLIB Addition

Allow applications via known hashes.

.008 Event Triggered Execution: Accessibility Features

Adversaries can replace accessibility features binaries with alternate binaries to execute this technique. Identify and block potentially malicious software executed through accessibility features functionality by using application control [1] tools, like Windows Defender Application Control[15], AppLocker, [2] [3] or Software Restriction Policies [16] where appropriate. [17]

.009 Event Triggered Execution: AppCert DLLs

Adversaries install new AppCertDLL binaries to execute this technique. Identify and block potentially malicious software executed through AppCertDLLs functionality by using application control [1] tools, like Windows Defender Application Control[15], AppLocker, [2] [3] or Software Restriction Policies [16] where appropriate. [17]

.010 Event Triggered Execution: AppInit DLLs

Adversaries can install new AppInit DLLs binaries to execute this technique. Identify and block potentially malicious software executed through AppInit DLLs functionality by using application control [1] tools, like Windows Defender Application Control[15], AppLocker, [2] [3] or Software Restriction Policies [16] where appropriate. [17]

Enterprise T1068 Exploitation for Privilege Escalation

Consider blocking the execution of known vulnerable drivers that adversaries may exploit to execute code in kernel mode. Validate driver block rules in audit mode to ensure stability prior to production deployment.[18]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

Limit or restrict program execution using anti-virus software. On MacOS, allowlist programs that are allowed to have the plist tag. All other programs should be considered suspicious.

.006 Hide Artifacts: Run Virtual Instance

Use application control to mitigate installation and use of unapproved virtualization software.

Enterprise T1574 Hijack Execution Flow

Adversaries may use new payloads to execute this technique. Identify and block potentially malicious software executed through hijacking by using application control solutions also capable of blocking libraries loaded by legitimate software.

.001 DLL

Identify and block potentially malicious software executed through DLL hijacking by using application control solutions capable of blocking DLLs loaded by legitimate software.[19]

.006 Dynamic Linker Hijacking

Adversaries may use new payloads to execute this technique. Identify and block potentially malicious software executed through hijacking by using application control solutions also capable of blocking libraries loaded by legitimate software.

.007 Path Interception by PATH Environment Variable

Adversaries will likely need to place new binaries in locations to be executed through this weakness. Identify and block potentially malicious software executed path interception by using application control tools, like Windows Defender Application Control, AppLocker, or Software Restriction Policies where appropriate.[20][15][2][3][21][22]

.008 Path Interception by Search Order Hijacking

Adversaries will likely need to place new binaries in locations to be executed through this weakness. Identify and block potentially malicious software executed path interception by using application control tools, like Windows Defender Application Control, AppLocker, or Software Restriction Policies where appropriate.[20][15][2][3][21][22]

.009 Path Interception by Unquoted Path

Adversaries will likely need to place new binaries in locations to be executed through this weakness. Identify and block potentially malicious software executed path interception by using application control tools, like Windows Defender Application Control, AppLocker, or Software Restriction Policies where appropriate.[20][15][2][3][21][22]

.012 COR_PROFILER

Identify and block potentially malicious unmanaged COR_PROFILER profiling DLLs by using application control solutions like AppLocker that are capable of auditing and/or blocking unapproved DLLs.[1][2][3]

Enterprise T1562 Impair Defenses

Use application control where appropriate, especially regarding the execution of tools outside of the organization's security policies (such as rootkit removal tools) that have been abused to impair system defenses. Ensure that only

approved security applications are used and running on enterprise systems.

.001 Disable or Modify Tools

Use application control where appropriate, especially regarding the execution of tools outside of the organization's security policies (such as rootkit removal tools) that have been abused to impair system defenses. Ensure that only approved security applications are used and running on enterprise systems.

.011 Spoof Security Alerting

Use application controls to mitigate installation and use of payloads that may be utilized to spoof security alerting.

Enterprise T1490 Inhibit System Recovery

Consider using application control configured to block execution of utilities such as `diskshadow.exe` that may not be required for a given system or network to prevent potential misuse by adversaries.

Enterprise T1674 Input Injection

Denylist scripting and use application control where appropriate. For example, PowerShell Constrained Language mode can be used to restrict access to sensitive or otherwise dangerous language elements such as those used to execute arbitrary Windows APIs or files (e.g., `Add-Type`).[9]

Enterprise T1036 Masquerading

Use tools that restrict program execution via application control by attributes other than file name for common operating system utilities that are needed.

.005 Match Legitimate Resource Name or Location

Use tools that restrict program execution via application control by attributes other than file name for common operating system utilities that are needed.

.008 Masquerade File Type

Ensure that input sanitization is performed and that files are validated properly before execution; furthermore, implement a strict allow list to ensure that only authorized file types are processed.[23] Restrict and/or block execution of files where headers and extensions do not match.

Enterprise T1106 Native API

Identify and block potentially malicious software executed that may be executed through this technique by using application control [1] tools, like Windows Defender Application Control[15], AppLocker, [2] [3] or Software Restriction Policies [16] where appropriate. [17]

Enterprise T1219 Remote Access Tools

Use application control to mitigate installation and use of unapproved software that can be used for remote access.

.001 IDE Tunneling

Use Group Policies to require user authentication by disabling anonymous tunnel access, preventing any unauthenticated tunnel creation or usage. Disable the Visual Studio Dev Tunnels feature to block tunnel-related commands, allowing only minimal exceptions for utility functions (unset, echo, ping, and user). Restrict tunnel access to approved Microsoft Entra tenant IDs by specifying allowed tenants; all other users are denied access by default.[24][25]

.002 Remote Desktop Software

Use application control to mitigate installation and use of unapproved software that can be used for remote access.

Enterprise T1505 .004 Server Software Component: IIS Components

Restrict unallowed ISAPI extensions and filters from running by specifying a list of ISAPI extensions and filters that can run on IIS.[26]

Enterprise T1129 Shared Modules

Identify and block potentially malicious software executed through this technique by using application control tools capable of preventing unknown modules from being loaded.

Enterprise T1176 Software Extensions

Set an extension allow or deny list as appropriate for your security policy.

.001 Browser Extensions

Set a browser extension allow or deny list as appropriate for your security policy.[27]

.002 IDE Extensions

Set an IDE extension allow or deny list as appropriate for your security policy.

Enterprise T1553 Subvert Trust Controls

System settings can prevent applications from running that haven't been downloaded through the Apple Store (or other legitimate repositories) which can help mitigate some of these issues. Also enable application control solutions such as AppLocker and/or Device Guard to block the loading of malicious content.

.001 Gatekeeper Bypass

System settings can prevent applications from running that haven't been downloaded through the Apple Store which can help mitigate some of these issues.

.003 SIP and Trust Provider Hijacking

Enable application control solutions such as AppLocker and/or Device Guard to block the loading of malicious SIP DLLs.

.005 Mark-of-the-Web Bypass

Consider blocking container file types at web and/or email gateways. Consider unregistering container file extensions in Windows File Explorer.[28]

Enterprise T1218 System Binary Proxy Execution

Consider using application control to prevent execution of binaries that are susceptible to abuse and not required for a given system or network.

.001 Compiled HTML File

Consider using application control to prevent execution of hh.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

.002 Control Panel

Identify and block potentially malicious and unknown .cpl files by using application control [1] tools, like Windows Defender Application Control[15], AppLocker, [2] [3] or Software Restriction Policies [16] where appropriate. [17]

.003 CMSTP

Consider using application control configured to block execution of CMSTP.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

.004 InstallUtil

Use application control configured to block execution of InstallUtil.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

.005 Mshta

Use application control configured to block execution of `mshta.exe` if it is not required for a given system or network to prevent potential misuse by adversaries. For example, in Windows 10 and Windows Server 2016 and above, Windows Defender Application Control (WDAC) policy rules may be applied to block the `mshta.exe` application and to prevent abuse.[29]

.008 Odbcconf

Use application control configured to block execution of Odbcconf.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

.009 Regsvcs/Regasm

Block execution of Regsvcs.exe and Regasm.exe if they are not required for a given system or network to prevent potential misuse by adversaries.

.012 Verclsid

Use application control configured to block execution of verclsid.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

.013 Mavinject

Use application control configured to block execution of mavinject.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

.014 MMC

Use application control configured to block execution of MMC if it is not required for a given system or network to prevent potential misuse by adversaries.

.015 Electron Applications

Where possible, enforce binary and application integrity with digital signature verification to prevent untrusted code from executing. For example, do not use `shell.openExternal` with untrusted content.

Where possible, set `nodeIntegration` to false, which disables access to the Node.js function.[30] By disabling access to the Node.js function, this may limit the ability to execute malicious commands by injecting JavaScript code.

Do not disable `webSecurity`, which may allow for users of the application to invoke malicious content from online sources.

Enterprise T1216 System Script Proxy Execution

Certain signed scripts that can be used to execute other programs may not be necessary within a given environment. Use application control configured to block execution of these scripts if they are not required for a given system or network to prevent potential misuse by adversaries.

.001 PubPrn

Certain signed scripts that can be used to execute other programs may not be necessary within a given environment. Use application control configured to block execution of these scripts if they are not required for a given system or network to prevent potential misuse by adversaries.

.002 SyncAppvPublishingServer

Certain signed scripts that can be used to execute other programs may not be necessary within a given environment. Use application control configured to block execution of these scripts if they are not required for a given system or network to prevent potential misuse by adversaries.

Enterprise T1080 Taint Shared Content

Identify potentially malicious software that may be used to taint content or may result from it and audit and/or block the unknown programs by using application control [1] tools, like AppLocker, [2] [3] or Software Restriction Policies [16] where appropriate. [17]

Enterprise T1127 Trusted Developer Utilities Proxy Execution

Certain developer utilities should be blocked or restricted if not required.

.001 MSBuild

Use application control configured to block execution of `msbuild.exe` if it is not required for a given system or network to prevent potential misuse by adversaries. For example, in Windows 10 and Windows Server 2016 and above, Windows Defender Application Control (WDAC) policy rules may be applied to block the `msbuild.exe` application and to prevent abuse.[29]

.003 JamPlus

Consider blocking or restricting JamPlus if not required.

Enterprise T1204 User Execution

Application control may be able to prevent the running of executables masquerading as other files.

.002 Malicious File

Application control may be able to prevent the running of executables masquerading as other files.

.004 Malicious Copy and Paste

Use application control where appropriate. PowerShell Constrained Language mode can be used to restrict access to sensitive or otherwise dangerous language elements such as those used to execute arbitrary Windows APIs or files (e.g., `Add-Type`).[9]

Enterprise T1047 Windows Management Instrumentation

Use application control configured to block execution of `wmic.exe` if it is not required for a given system or network to prevent potential misuse by adversaries. For example, in Windows 10 and Windows Server 2016 and above, Windows Defender Application Control (WDAC) policy rules may be applied to block the `wmic.exe` application and to prevent abuse.[29]

Enterprise T1220 XSL Script Processing

If msxsl.exe is unnecessary, then block its execution to prevent abuse by adversaries.
