Windows 10 22H2 Security Baseline

Microsoft is pleased to announce the release of the security baseline package for Windows 10, version 22H2!

Please download the content from the Microsoft Security Compliance Toolkit, test the recommended configurations, and customize / implement as appropriate.

This release includes numerous changes to further assist in the security of enterprise customers. Changes have been made for additional protections around driver security, credential theft, printers, and account lockout.

Printers

- Support for **RedirectionGuard** is added to the print service. RedirectionGuard is a security measure that prevents the use of non-administratively created redirection primitives from being followed within a given process. The setting **Configure Redirection Guard** is now **Enabled** as part of the baseline.
- **Manage processing of queue-specific files** (also called **CopyFilesPolicy**) was first introduced as a registry key in response to CVE-2021-36958 in September of 2021. This setting allows standard color profile processing using the inbox mscms.dll executable and nothing else. The security baseline is to configure this setting to **Enabled** with the option of **Limit queue-specific files to color profiles**. For Windows 10, version 22H2 this setting is not yet available natively, therefore we have created the setting and added it to the SecGuide.ADMX.
- **Limit print driver installation to Administrators** was introduced to the security baselines as part of the SecGuide.ADMX before an inbox policy was available. This policy is now contained within the OS, and the MS Security Guide setting is deprecated. However, since both settings write to the same location, the configured values still appear in both locations. The explanatory text in the MS Security Guide is updated to point users to the new location.
- **Configure RPC packet level privacy setting for incoming connections** has been added to SecGuide.ADMX as a result of CVE-2021-1678 and is set to **Enabled** as part of the baseline. The work of creating and deploying registry keys is now included in the security baseline until the setting becomes inbox to Windows.

Credential Theft Protection

Additional Local Security Authority (LSA) protection provides defense by running LSA as a protected process. LSA protection was first introduced in the Windows 8.1 security baseline, as part of the original Pass-the-Hash mitigations. At this time the security baseline will move MS Security Guide\LSA Protection to a value of enabled.

Attack Surface Reduction

A new rule **Block abuse of exploited vulnerable signed drivers** is now included as part of the operating system baselines as part of the Microsoft Defender Antivirus GPO. This rule applies across both client and server and helps prevent an application from writing a vulnerable signed driver to disk.

For additional information, see the topic Attack surface reduction rules reference | Microsoft Docs.

Account Lockout Policies

A new policy **Allow Administrator account lockout**, located under `Security Settings\Account Policies\Account Lockout Policy` is added to mitigate brute-force authentication attacks. The recommended values for the policies **Account lockout duration** and **Reset account lockout counter after** are adjusted to be consistent with the defaults for out-of-the-box Windows installations.

Other Changes

Corrected in this release was a mismatch between the security baseline documentation and the accompanying Group Policy for Microsoft Defender Antivirus settings. The documentation stated that `Windows Components\Microsoft Defender Antivirus\Real-time Protection\Turn on behavior monitoring` should be set to **Enabled**, but the actual GPO remained in a **Not Configured** state. This is corrected in this release.

Please let us know your thoughts by commenting on this post or through the Security Baseline Community.