Changes in the Security Guidance for Windows 8.1, Server 2012 R2 and IE11 since the beta

We have made a small number of changes in the baseline security guidance for Windows 8.1, Windows Server 2012 R2 and Internet Explorer 11 since we released the beta version of our guidance last April. This blog post discusses those changes and the reasons for them.

**Account Lockout Threshold:** we’re changing the incorrect-password threshold that triggers account lockout from “5” in the beta to “10”. Account lockout is an involved and controversial setting, so we discuss the thinking behind this setting in a separate blog post. *[add hyperlink]* This change applies to all supported versions of Windows.

**Include command line in process creation events**: The beta guidance recommended enabling this setting in Computer Configuration\Administrative Templates\System\Audit Process Creation. We are reverting that recommendation back to “Not Configured”. The original idea for the previous recommendation was to make more information available for forensic purposes. The command line data being logged is captured in the Security event log, which requires administrative or admin-equivalent privilege to read, and administrators have many other ways to capture full command line data and much more from running systems, so in our initial estimate the guidance assumed that there was minimal security risk to capture full command lines in process creation audit events. However, although it’s certainly discouraged, command lines such as NET.EXE USE and PsExec often contain passwords and other sensitive information, and logging those command lines could make months of such captured data available to an attacker the instant they compromise a machine. For this reason we are reverting the recommendation back to “Not configured”; the resulting default behavior is not to include the command line in the audit events. By not explicitly recommending “Disabled”, organizations can still enable the policy when situations dictate. This change applies to Windows 8.1 and Server 2012 R2.

**Disabling Digest Authentication**: Digest Authentication, documented in RFCs 2617 and 2831, is a standards-based authentication protocol that was intended to improve upon earlier authentication protocols such as Basic Authentication by using a challenge/response mechanism to prove knowledge of a password instead of sending the password to the remote server. The Windows implementation (often called WDigest) provided single-sign-on support for Digest Authentication by default. This support required that Lsass.exe retain an encrypted copy of the user’s password in memory so that it could be decrypted and used whenever needed without having to prompt the user. External security researchers reverse-engineered Lsass.exe’s behavior and determined how to extract the decrypted password. Because Digest Authentication is not widely used and to help prevent credential theft, Windows disabled Digest Authentication by default beginning in Windows 8.1 and Windows Server 2012 R2 and created a registry setting to control whether Digest is enabled. With the release of KB 2871997, that same setting is now available for earlier versions of Windows going back to Windows 7 and Windows Server 2008 R2. However, installing the update does not disable Digest on those systems. The final version of the security guidance for Windows 8.1 and Server 2012 R2 includes an additional entry to the custom “SCM: Pass the Hash Mitigations” ADMX so that Digest can be disabled through Group Policy on all versions of Windows going back to Windows 7 and Server 2008 R2.

**EMET 5.0**: Version 5.0 of the Enhanced Mitigation Experience Toolkit was released between the beta and final versions of this security guidance. We have replaced the EMET 4.1 policy settings from the beta with the corresponding EMET 5.0 policy settings, which are almost identical. EMET 5.0 can be downloaded from <http://www.microsoft.com/emet>.

**Deny access to this computer from the network / Deny log on through Remote Desktop Services**: the recommendation to set these deny-logon rights to Guests and Local Account remains true for Windows 8.1 and Server 2012 R2. With the release of KB 2871997, “NT AUTHORITY\Local Account” is now defined on Windows 7, Windows 8, Server 2008 R2 and Server 2012, so the guidance applies there as well. We also recommend adding your Domain Admins and Enterprise Admins to these deny-logon rights for all versions of Windows except for domain controllers and for dedicated administrative workstations.

**Bypass traverse checking privilege**: If a user requests access to a file, directory or registry key and does not possess this privilege, Windows checks not only the permissions on the requested object but also verifies that the user has “traverse” permissions on parent keys or directories all the way up to the root container, which can incur significant performance penalties. This is a security “feature” available since Windows NT 3.1 that no one has ever wanted. Windows grants this privilege – internally called SeChangeNotifyPrivilege – to Everyone by default, as well as to BUILTIN\Users and several other groups (although one would think “Everyone” would be all-encompassing enough). The Local Security Policy editor and KB 823659 (<http://support.microsoft.com/kb/823659>) warn that changing the defaults can cause serious problems. Nevertheless, security guidance from Microsoft and others has long recommended removing “Everyone” from the list. This probably ends up having little effect, as BUILTIN\Users is a very broad group. Rather than try to continue to track the other default grantees, such as “Windows Manager\Windows Manager Group” which was added to the list in Windows 8, we recommend not defining an explicit value and instead allowing the out-of-the-box default to remain in place.

The only scenario in which this could be a problem is if a caller who is a member of Everyone but not of Users (unusual enough in itself) is able to request access to a file or registry key, and the permissions on the object allow the request, but it’s in a directory or key hierarchy that does not grant the user the Traverse permission all the way to the top – AND that the expected behavior would be to deny access. This is too unusual a scenario to consider a security risk. If the expected behavior is to deny access, don’t grant non-Users access to the requested resources.

**Increase a process working set privilege**: A process’ “working set” is the amount of physical memory assigned to the process by the memory manager. We are removing the guidance that has recommended granting this privilege only to Administrators and Local Service; instead we recommending leaving this privilege at the operating system default value. On Windows 7 the default is “Users”; on Windows 8 and newer it is also granted to “Window Manager\Window Manager Group”. Because future versions of Windows may change the value again, we recommend not defining an explicit value and instead allowing the out-of-the-box default to remain in place.

The existing Threats and Countermeasures text for the privilege says, “It would be possible for malicious code to increase the process working set to a level that could severely degrade system performance and potentially cause a denial of service.” However, any process that does not have memory quotas applied to it can always allocate memory and then page it into the working set simply by accessing it. The “Increase…” privilege grants only the ability for a process to call certain APIs that request specific minimum and maximum working set sizes; however, even if the APIs report success, Windows does not guarantee that the request will be honored. Removing the privilege from Users can cause application compatibility problems for programs that expect to have the privilege, while providing no real security benefit.

This change should be applied to all versions of Windows.

**Increase event log sizes on Windows client**: We are increasing the maximum log file sizes for the Application, Security and System event logs for Windows client to match the sizes for Windows Server. The log file sizes had been left at the default 20480 KB; we are changing them to 32768 KB for the Application and System event logs, and 196608 KB for the Security event log. It makes sense to take advantage of increasing storage to increase diagnostic and forensic capabilities. This change should be applied to all Windows client versions.

**Apply UAC restrictions to local accounts on network logons (LocalAccountTokenFilterPolicy)**: We are removing this setting from the Domain Controller baseline because it does not have meaning on domain controllers. It remains in the Windows client and Member Server baselines.

**Access this computer from the network**: On Windows client, we are changing this from Adminstrators and Users to Administrators and Authenticated Users, to make it consistent with the Member Server baselines. This change does not have significant security implications.

**Specify the search server for device driver updates**: We are reverting this setting in Computer Configuration\Administrative Templates\System\Device Installation to “Not configured” because configuration is organization-specific and depends upon whether the organization has an internal server to host driver updates.