CIS Microsoft Windows Server 2012 R2 v2.2.0 (v2.2.1)

Check: 1.2.3 Is the 'Reset account lockout counter after' parameter set to '15 or more minute(s)'? 2

Status and evidence as reported by CCS: 2

Issue: Check has wrong expression 2

Fix: Expression should use “>=” instead of “=” 2

Check: 18.4.13.1 (18.4.14.1) Is the 'Hardened UNC Paths' parameter set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'? 2

Status and evidence as reported by CCS: 2

Setting on server: 3

Issue: 3

Fix: 3

Check: 18.9.22.3 (18.9.24.3) Is the 'Default Protections for Internet Explorer' parameter set to 'Enabled'? 4

Status and evidence as reported by CCS: 4

Setting on server: 4

Issue: 4

Fix: 4

Check: 18.9.22.4 (18.9.24.4) Is the 'Default Protections for Popular Software' parameter set to 'Enabled'? 4

Status and evidence as reported by CCS: 4

Setting on server: 5

Issue: 5

Fix: 5

Check: 18.9.22.5 (18.9.24.5) Is the 'Default Protections for Recommended Software' parameter set to 'Enabled'? 5

Status and evidence as reported by CCS: 5

Setting on server: 5

Fix: 5

Check: 18.9.24.4.2 (18.9.26.4.2) Is the 'System: Specify the maximum log file size (KB)' parameter set to 'Enabled: 32,768 or greater'? 6

Status and evidence as reported by CCS: 6

Setting on server: 6

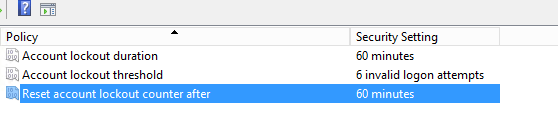
Issue: 6

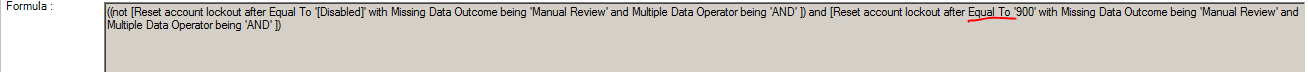
Fix: 6

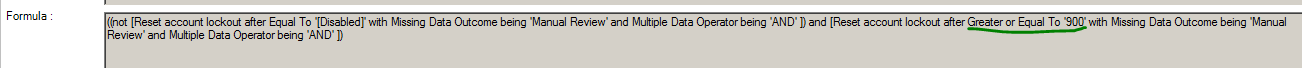
# Check: 1.2.3 Is the 'Reset account lockout counter after' parameter set to '15 or more minute(s)'?

## Status and evidence as reported by CCS:

|  |  |  |  |
| --- | --- | --- | --- |
| Check Name | Status | Risk Score | Evidence |
| 1.2.3 Is the 'Reset account lockout counter after' parameter set to '15 or more minute(s)'? | Fail... | 3.799999952 | Object Name: WORKGROUP\\GOLDV8W2K12 Object Type: Machines Expression: Reset account lockout after = '900' Current Value: 01:00:00 |

Setting on server:

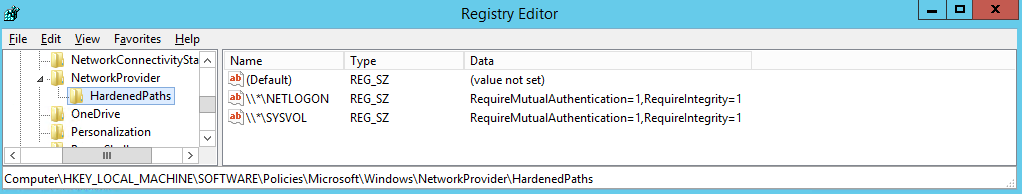
Issue: Check has wrong expression  
 

Fix: Expression should use “Greater or equal to” instead of “Equal to”  


# Check: 18.4.13.1 (18.4.14.1) Is the 'Hardened UNC Paths' parameter set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'?

## Status and evidence as reported by CCS:

|  |  |  |  |
| --- | --- | --- | --- |
| Check Name | Status | Risk Score | Evidence |
| 18.4.13.1 Is the 'Hardened UNC Paths' parameter set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'? | Fail... | 6.900000095 | Object Name: [No data available] Object Type: Registry Expression: Wnt.Registry.REGISTRYDATATYPEUSINGWMI = 'reg\_sz' Current Value: [No data available]  Object Name: [No data available] Object Type: Registry Expression: Wnt.Registry.REGISTRYVALUEUSINGWMI =~ '[Rr]equire([Mm]utual[Aa]uthentication|[Ii]ntegrity)=1.\*[Rr]equire([Mm]utual[Aa]uthentication|[Ii]ntegrity)=1' Current Value: [No data available] |

Setting on server:  


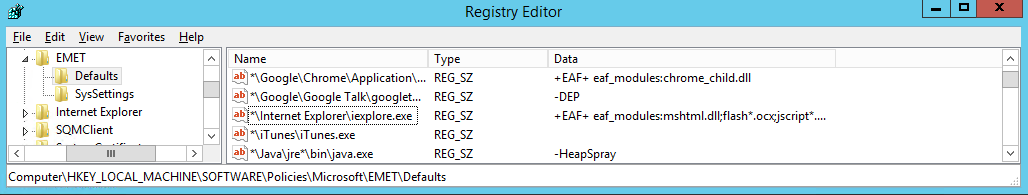
Issue:  
Original check logic has trouble reading unusual registry value name like "\\\*\SYSVOL".

Fix:  
Re-write check to use *Key/Value Name Matches Pattern* instead of *Value Name Equal To* inside Data Item Filter:  
“Key/Value Name Matches Pattern '/^HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows\\NetworkProvider\\HardenedPaths\\.\*SYSVOL$/”

# Check: 18.9.22.3 (18.9.24.3) Is the 'Default Protections for Internet Explorer' parameter set to 'Enabled'?

|  |  |  |  |
| --- | --- | --- | --- |
| Check Name | Status | Risk Score | Evidence |
| 18.9.22.3 Is the 'Default Protections for Internet Explorer' parameter set to 'Enabled'? | Fail... | 6.800000191 | Object Name: [No data available] Object Type: Registry Expression: Wnt.Registry.REGISTRYDATATYPEUSINGWMI = 'reg\_sz' Current Value: [No data available] |

## Status and evidence as reported by CCS:

Setting on server:  


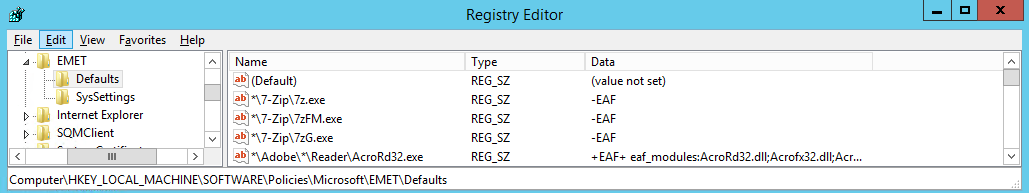
Issue:  
Original check logic has trouble reading unusual registry value name like " \*\Internet Explorer\iexplore.exe". On top of that, original checks does not verify if registry value data matches.

Fix:  
Re-write check to use *Key/Value Name Matches Pattern* instead of *Value Name Equal To* inside Data Item Filter: Key/Value Name Matches Pattern '/^HKLM\\Software\\Policies\\Microsoft\\EMET\\Defaults\\.\*Internet Explorer.\*iexplore.exe$/i'

# Check: 18.9.22.4 (18.9.24.4) Is the 'Default Protections for Popular Software' parameter set to 'Enabled'?

## Status and evidence as reported by CCS:

|  |  |  |  |
| --- | --- | --- | --- |
| Check Name | Status | Risk Score | Evidence |
| 18.9.22.4 Is the 'Default Protections for Popular Software' parameter set to 'Enabled'? | Fail... | 6.800000191 | Object Name: [No data available] Object Type: Registry Expression: Wnt.Registry.REGISTRYDATATYPEUSINGWMI = 'reg\_sz' Current Value: [No data available] |

Setting on server:  


Issue:  
Original check logic has trouble reading unusual registry value name like " \*\7-Zip\7z.exe". On top of that, original checks does not verify if registry value data matches.

Fix:  
Re-write check to use *Key/Value Name Matches Pattern* instead of *Value Name Equal To* inside Data Item Filter: Where Key/Value Name Matches Pattern '/^HKLM\\Software\\Policies\\Microsoft\\EMET\\Defaults\\.\*7-Zip.\*7z.exe$/'  
NOTE: not all registry values are covered here, only the first one, but the pattern to fix all is the same.

# Check: 18.9.22.5 (18.9.24.5) Is the 'Default Protections for Recommended Software' parameter set to 'Enabled'?

## Status and evidence as reported by CCS:

|  |  |  |  |
| --- | --- | --- | --- |
| Check Name | Status | Risk Score | Evidence |
| 18.9.22.5 Is the 'Default Protections for Recommended Software' parameter set to 'Enabled'? | Fail... | 6.800000191 | Object Name: [No data available] Object Type: Registry Expression: Wnt.Registry.REGISTRYDATATYPEUSINGWMI = 'reg\_sz' Current Value: [No data available] |

## Setting on server:

Issue:  
Original check logic has trouble reading unusual registry value name like " \*\Adobe\\*\Reader\AcroRd32.exe". On top of that, original checks does not verify if registry value data matches.

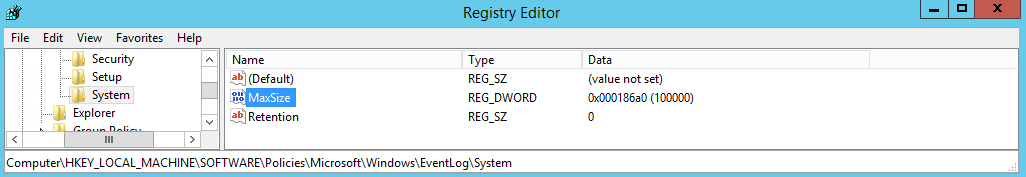
## Fix:

Re-write check to use *Key/Value Name Matches Pattern* instead of *Value Name Equal To* inside Data Item Filter: Where Key/Value Name Matches Pattern ' '/^HKLM\\Software\\Policies\\Microsoft\\EMET\\Defaults\\.\*Adobe.\*Reader.\*AcroRd32.exe$/'  
NOTE: not all registry values are covered here, only the first one, but the patters to fix all is the same.

# Check: 18.9.24.4.2 (18.9.26.4.2) Is the 'System: Specify the maximum log file size (KB)' parameter set to 'Enabled: 32,768 or greater'?

## Status and evidence as reported by CCS:

|  |  |  |  |
| --- | --- | --- | --- |
| Check Name | Status | Risk Score | Evidence |
| 18.9.24.4.2 Is the 'System: Specify the maximum log file size (KB)' parameter set to 'Enabled: 32,768 or greater'? | Fail... | 3.799999952 | Object Name: HKLM\Software\Policies\Microsoft\Windows\EventLog\System\MaxSize Object Type: Registry Expression: Wnt.Registry.REGISTRYVALUEUSINGWMI >= '32768' Current Value: 100000 |

Setting on server:  


Issue:  
Some bug in WMI registry check that caused it not to recognize values properly.

Fix:  
Change Value >= '32768' to Value as DWORD Greater or Equal To '32768'