McAee TIE and ATP Rule Content Update 978

Release Notes: 2019-08-21

Below is the new/modified rule information for McAfee Threat Intelligence Exchange and ATP Rule content update

New Rules

Rule 332 – Prevent certutil.exe from downloaded files

Description: CertUtil is a binary that can be abused by attackers to fetch remote payloads. This rule prevents syntax allowing cert util to fetch payloads remotely

Default State: Evaluate / On (only in HighSecurity)

Changes in this release: New rule to detect certutil.exe being abused

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions

Updated Rules

Rule 260 – Detect AMSI bypass techniques

Description: Detect the techniques which are used to bypass Antimalware Scan Interface (AMSI)

Default State: Evaluate

Changes in this release: Improved logic more detection effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions

Rule 258 – Detect masqueraded files or process launches

Description: Alerts on if a common system file is renamed or dropped in a non-standard location

Default State: Evaluate

Changes in this release: Improved logic fore more detection effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions

Rules That Changed Exposure or Security Posture:

Rule 257 – Detect potentially malicious usage of WMI"

Description: Looks for common usage of wmi to either execute remote code, move laterally or persist

Changes in this release: Evaluate to Evaluate / On (only in HighSecurity)

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions

Rule 255 – Detect potentially obfuscated command line parameters

Description: Trigger on command line arguments that are highly obfuscated

Changes in this release: Default On to Evaluate / On (only in HighSecurity)

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions

Notes:

For more information refer the KB82925.