McAee TIE and ATP Rule Content Update 924

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

New Rules

None

Updated Rules

Rule 258 – Detect masqueraded files or process launches

Description: Aggressively blocks processes where files have been renamed (such as script interpreters)

Default State: Evaluate

Changes in this release: Improve in Detection Effectiveness

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: This rule is designed to analyze command line parameters passed to programs to alert on potentially obfuscated strings that could indicate malicious behavior

Default State: On

Changes in this release: Improve in 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

Changed State: Evaluate

Changes in this release: Also covers disconnected environments

Affected Products:

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

Rule 256 – Detect use of long -encodedcommand powershell

Changed State: Evaluate

Changes in this release: Also covers disconnected environments

Affected Products:

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

Rule 139 – Identify trusted DOTNet assemblies

Changed State: Mandatory

Changes in this release: Reputation changed to assumed clean

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan
- ✓ WSS

Rule 138 – Identify trusted unsigned Microsoft DOTNet assemblies

Changed State: On

Changes in this release: Rule exposure changed from GTI connectivity to Disconnected state. Reputation changed to assumed clean

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan
- ✓ WSS

Rule 137 – Identify unsigned DOTNet assemblies that Might Be Trusted

Changed State: On

Changes in this release: Rule exposure changed from GTI connectivity to Disconnected state. Reputation changed to assumed clean

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan
- ✓ WSS

Rule 136 – Identify unsigned NativeImage Files that Might Be Trusted

Changed State: On

Changes in this release: Rule exposure changed from GTI connectivity to Disconnected state. Reputation changed to assumed clean

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan
- ✓ WSS

Notes:

For more information refer the KB82925.