Threat Intelligence Exchange Rule Content Update 855

Release Notes: 2019-02-14

Below is the new/modified rule information for McAfee Threat Intelligence Exchange

New Rules

None

Updated Rules

Rule 243 – Identify and block suspicious process executions

Description: This rule identifies and blocks suspicious execution of a process in an application by giving dirty reputation

Default State: Evaluate

Changes in this release: Improve detection effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ WSS 15.x, 16.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

Changes in this release: Improve detection effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ WSS 16.x versions

Rule 307 – Identify suspicious payloads targeting Network related services or applications

Description: Identify suspicious payloads targeting Network related services or applications and will not allow launch of tools which indicate suspicious behavior

Changes in this release: Improve detection effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ WSS 16.x versions

Rule 321 – Prevent cmd.exe from launching any process with an unknown reputation

Description: Attempts to prevent suspicious process chains by keeping cmd from further spawning script interpreting processes

Changes in this release: Improve detection effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ WSS 16.x versions

Rules That Changed Exposure or Security Posture:

None

Notes:

For more information refer the KB82925.