Threat Intelligence Exchange and ATP Rule Content 893
Release Notes

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

New Rules

Rule 257 – Detect potentially malicious usage of WMI

Description: WMI provides a way of executing code or moving laterally in an environment. Some legitimate software may use this so this rule should be baselined in your environment

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 326 – Identify suspicious payloads invoking Rundll32 in high change systems

Description: Identify highly suspicious payloads abusing Rundll32 in high change systems

Default State: Evaluate / On (only in HighSecurity)

Changes in this release: Improve in Detection Effectiveness

Affected Products:

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

Updated Rules

Rule 239 – Prevent cmd.exe from launching other script interpreters such as cscript or powershell in all rule group assignments

Description: Block dual use tools from being launched by cmd. that are commonly used in attacks

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
- ✓ WSS 15.x, 16.x versions
- ✓ Threat Intelligence Exchange for Virus Scan

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 in Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ WSS 15.x, 16.x versions
- ✓ Threat Intelligence Exchange for Virus Scan

Rule 327 – Identify most probable suspicious payloads invoking rundll32 process

Description: Identify most probable suspicious payloads invoking rundll32 process

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

Rules That Changed Exposure or Security Posture:
None

Notes:
For more information refer the KB82925.