McAee TIE and ATP Rule Content Update 908
Release Notes

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

New Rules

Rule 330 – Identify and block probably suspicious invoking of system process SvcHost and hence preventing it from abuse

Description: L"Looks for any potentially malicious invoking of SvcHost system process and blocks it from undesired process injections from unknown actor process's"

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 329 – Identify and block suspicious usage of Scheduled Tasks in high change systems"

Description: Looks for any potentially malicious invoking of schedule tasks and blocks them before being added in high change systems. This will attempt to cut off malware persistence mechanism

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

Rule 313 – Prevent various text editors like notepad and wordpad from spawning processes that can execute script commands in all rule group assignments

Description: Keep text editors from being used to spawn processes like cmd or powershell

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

Rule 258 – Detect masqueraded files or process launches

Description: This rule looks for scenarios 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
- ✓ Threat Intelligence Exchange for Virus Scan

Updated Rules

Rule 315 – Aggressively blocks processes with unknown reputations from being spawned by text editors

Description: Aggressively blocks processes with unknown reputations from being spawned by text editors like notepad, word pad etc

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 309 – Block processes attempting to launch from office applications. Rule enabled only in high security policies

Description: Attempts to prevent office applications from being abused to deliver malicious payloads when it is enabled to systems with a high security policies

Default State: On/Evaluate(High ChangeSystems)

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 221 – L"Identify new suspicious files seen on a small number of systems"

Changed State: Evaluate to OFF

Changes in this release: Removed the rule as the detection logic is covered in more advanced rules

Affected Products:

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

Rule 236 – L"Identify new suspicious files seen on a small number of LAM systems"

Changed State: Evaluate to OFF

Changes in this release: Removed the rule as the detection logic is covered in more advanced rules

Affected Products:

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

Rule 241 – L" Identify new suspicious files seen on a small number of systems (v2)”

Changed State: Evaluate to OFF

Changes in this release: Removed the rule as the detection logic is covered in more advanced rules

Affected Products:

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

Rule 246 – L" Identify new suspicious files seen on a small number of systems (v3)”

Changed State: Evaluate to OFF

Changes in this release: Removed the rule as the detection logic is covered in more advanced rules

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.