Threat Intelligence Exchange Rule Content Update 767

Release Notes: 2018-09-06

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

New Rules

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 in Security mode and Evaluate in Productivity/Balanced mode

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 312 – Aggressively blocks any process with an unknown reputation from being spawned by e-mail clients

Description: This rule is more aggressive at blocking processes that seem suspect when spawning under e-mail clients

Default State: Evaluate

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

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

Description: This rule is more aggressive at blocking processes that seem suspect when spawning under text editors

Default State: Evaluate

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 317 – Prevent PDF readers from launching processes that can execute scripts in Security rule group assignments only

Description: Prevent PDF readers from launching processes that can execute scripts

Default State: On in Security mode and Evaluate in Productivity/Balanced mode

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 318 – Aggressively prevent PDF readers from launching processes with an unknown reputation

Description: Aggressively prevent PDF readers from launching processes with an unknown reputation

Default State: Evaluate

Affected Products:

- ✓ Endpoint Security ENS 10.6.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

Default State: Evaluate

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 324 – Prevent mshta from launching suspicious process

Description: Prevent mshta from launching any suspicious process

Default State: Evaluate

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 327 – Identify most probable suspicious payloads invoking rundll32 process

Description: Identify suspicious payloads invoking Rundll32 process

Default State: Evaluate

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Updated Rules

Rule 300 – Prevent office applications from launching child processes that can execute script commands

Description: Prevent office applications from launching children processes that can execute scripts like powershell and cscript

Default State: On

Changes in this release: Improved Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 301 – Aggressively blocks processes with unknown reputations from being spawned by office applications

Description: This has some rules that are more aggressive at stopping processes attempting to abuse office applications

Default State: Evaluate

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 303 – Identify highly suspicious payloads targeting Browser related applications

Description: Identify highly suspicious payloads including unknown binaries targeting Browser applications like Firefox, Chrome, Edge and Others.

Default State: On

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 304 – Identify suspicious payloads targeting Browser related applications

Description: Identify most probable suspicious payloads targeting Browser applications.

Default State: Evaluate

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

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

Description: Identify most probable suspicious payloads targeting Network related services or applications

Default State: Evaluate

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rules That Changed Exposure or Security Posture:

None.

Notes:

For more information refer the KB82925