Threat Intelligence Exchange Rule Content Update 771

Release Notes: 2018-10-04

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

New Rules

None

Updated 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

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 314 – Prevent various text editors like notepad and wordpad from spawning processes that can execute script commands in Security rule group assignment

Description: Prevent text editors from spawning new processes that can further be used to execute scripting commands in the Security rule group assignment

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

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 316 – Prevent PDF readers from launching processes that can execute scripts in all rule group assignments

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

Default State: On

Changes in this release: Improve Detection Effectiveness

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 in Security rule group assignments only

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

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rules That Changed Exposure or Security Posture:

Rule 250 – Elevate trust of a file which got scanned multiple times without detection

Description: Elevate trust of a file based on local age on disk when the file has been scanned multiple times and has no suspicious characteristics

Default State: On

Changes in this release: Improve Trust on clean files

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

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: GTIConnectivity required

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Notes:
For more information refer the KB82925