McAfee TIE and ATP Rule Content Update 1472

Below is the new/modified rule information for McAfee TIE and ATP Rule Content Update

New Rules

None

Updated Rules

Rule 301: Blocks cmd.exe from being spawned by office applications

Description: This rule prevents office applications from being used to spawn processes like cmd

Default State: Evaluate

Changes in this release: Improve detection effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x, 10.7.x versions

Rule 513: Detect commands used for copying files from a remote system

Description: Block remote copy operations or lateral tool operations from external environment. This rule can generate false positives, hence meant for highly restrictive environments (Tactic: Command and Control - Technique: T1105, T1570)

Default State: Off

Changes in this release: Improve detection effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x, 10.7.x version

Rules That Changed Exposure or Security Posture:

None

Notes:

For more information refer the KB82925.