Threat Intelligence Exchange Rule Content Update 661

Release Notes: 2017-05-22

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

New Rules

Rule 58 – Identify trust for files executed on network shares

Description: identify trust for files executed on network shares using file attributes and other related information like prevalence

Default State: Evaluate

Changes in this release: New rule to identify trust for files executed on network shares using scanner results and file attributes to indicate trust

Affected Products:

- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan
- ✓ Cloud-AV
- ✓ WSS 15.x versions

Updated Rules

Rule 205 – Identify suspicious files that have odd creation dates and are likely not packed

Description: Identifies suspicious files that are likely not packed, have odd creation dates, and are in locations such as the Temp or Downloads folders

Default State: Evaluate

Changes in this release: Updated algorithm to improve detection effectiveness

Affected Products:

- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan
- ✓ Cloud-AV
- ✓ WSS 15.x versions

Rule 209 – Identify suspicious files that are hidden from the user

Description: Identifies suspicious files that are executed or loaded while hidden from the user

Default State: On

Changes in this release: Updated algorithm to improve detection effectiveness

Affected Products:

- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan
- ✓ Cloud-AV
- ✓ WSS 15.x versions

Rule 219 - Identify a suspicious file that hides in a secure location

Description: Identifies files in secure locations, such as folders reserved for system drivers. These files are not consistent with other files in that location and have suspicious characteristics

Default State: On

Changes in this release: Updated algorithm to improve detection effectiveness

Affected Products:

- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan
- ✓ Cloud-AV
- ✓ WSS 15.x versions

Rule 221 - Identify new suspicious files seen on a small number of systems

Description: Detects files that originated from an externally-facing application (a network-aware application that downloads files). These are newly discovered files in the environment and have characteristics and import functions that indicate they are suspicious

Default State: Evaluate

Changes in this release: Updated algorithm to improve detection effectiveness

Affected Products:

- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan

Rule 236 - Identify new and suspicious files seen on a small number of systems

Description: Detects files that originated from an externally-facing application (a network-aware application that downloads files). These are newly discovered files in the environment and have characteristics and import functions that indicate they are suspicious

Default State: Evaluate

Changes in this release: Updated algorithm to improve detection effectiveness

Affected Products:

- ✓ Cloud-AV
- ✓ WSS 15.x versions

Rule 241 - Identify new suspicious files seen on a small number of systems (v2)

Description: This will detect new files that are seen on a small percentage of systems that have various characteristics and system locations that are indicative of suspicious behavior

Default State: Evaluate

Changes in this release: Updated algorithm to improve detection effectiveness

Affected Products:

- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan

Rule 246 - Identify new suspicious files seen on a small number of systems (v3)

Description: This will detect new files that are seen on a small percentage of systems that have various characteristics and system locations that are indicative of suspicious behavior

Default State: Evaluate

Changes in this release: Updated algorithm to improve detection effectiveness

Affected Products:

- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan

Rules That Changed Exposure or Security Posture:

None.

Notes:

None.