Threat Intelligence Exchange Rule Content Update 682

Release Notes: 2017-07-22

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

New Rules

Rule 95 – Identify files that are signed by certificate of known clean reputation and mark them Most Likely Trusted when offline

Description: Identifies files that are signed by certificate of known clean reputation and mark them Most Likely Trusted when there is no TIE or GTI connectivity

Default State: On

Changes in this release: New Rule to identify trusted signed files when in offline mode

Affected Products:

- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan
- ✓ Cloud-AV
- ✓ WSS 15.x, 16.x versions

Rule 125 – Identify files marked as Trusted Windows AppStore Applications

Description: This rule identifies files that are marked as trusted Windows AppStore Applications based on the file attributes, file location and process attributes

Default State: Evaluate

Changes in this release: New Rule to identify files that are trusted Windows AppStore Applications

Affected Products:

- ✓ Endpoint Security 10.5.x versions

Updated Rules

Rule 1 – Use certificate reputation to identify trusted or malicious files

Description: This rule determines if a file is trusted or malicious based on the GTI or Enterprise reputation of the signing certificate. The certificate reputation must be Known Malicious, Known Trusted, Most Likely Malicious, or Most Likely Trusted

Default State: Mandatory

Changes in this release: Address issue causing excessive queries to the TIE server in TIE-connected environments

Affected Products:

- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan
- ✓ Cloud-AV
- ✓ WSS 15.x, 16.x versions

Rule 133 – Identify trusted files on the disk

Description: Identifies files that are present on the disk and are not suspicious before installing the TIE module

Default State: Mandatory

Changes in this release: Fix Rule logic 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, 16.x versions

Rule 134 – Identify trusted files on the disk that were prevalent in the enterprise prior to installing the TIE module

Description: Identifies files that are present on the disk and are not suspicious before installing the TIE module and have been seen in the enterprise

Default State: Mandatory

Changes in this release: Fix Rule logic 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, 16.x versions

Rule 57 – Use GTI file reputation to identify files that Might be Trusted or Might be Malicious

Description: Determines files which Might be Trusted or Might be Malicious based on GTI file reputation

Default State: On

Changes in this release: Fix Rule logic 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, 16.x versions

Rules That Changed Exposure or Security Posture:

None.

Notes:

None.