

## Threat Intelligence Exchange Rule Content Update 623

Release Notes: 2017-01-31

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

### New Rules

**Rule 251** – Identify files that MWG reports as suspicious

**Description:** Identifies files that McAfee Web Gateway reports as Known Malicious or Most Likely Malicious and issues a Most Likely Malicious reputation.

**Default State:** Evaluate

**Changes in this release:** New algorithm to identify files reported as suspicious by MWG

**Affected Products:**

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

### Updated Rules

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

**Description:** Determines if a file is trusted or malicious based on the GTI or Enterprise reputation of the signing certificate

**Default State:** Mandatory

**Changes in this release:** Updated algorithm to improve product safety

**Affected Products:**

- ✓ Endpoint Security 10.1,10.2 and 10.5 versions
- ✓ Cloud-AV
- ✓ WSS 15.1
- ✓ Threat Intelligence Exchange for Virus Scan

**Rule 97** – Trust files based on typical systems security level when offline

**Description:** Determines that files with no suspicious characteristics are trusted when the system is offline (disconnected from the TIE server and from GTI).

**Default State:** Enabled

**Changes in this release:** Updated algorithm to improve detection effectiveness

**Affected Products:**

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

**Rule 98 – Trust files based on High Change Systems security level when offline**

**Description:** Determines that files with no suspicious characteristics are trusted when the system is offline (disconnected from the TIE server and from GTI)

**Default State:** Enabled

**Changes in this release:** Updated algorithm to improve detection effectiveness.

**Affected Products:**

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

**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:** Updated algorithm to improve detection effectiveness.

**Affected Products:**

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

**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:** Updated algorithm to improve detection effectiveness.

**Affected Products:**

- ✓ Endpoint Security 10.1,10.2 and 10.5 versions



- ✓ Threat Intelligence Exchange for Virus Scan

**Rule 244** – Use GTI file reputation to identify files that Might be Malicious seen on a small number of systems

**Description:** Determines files which Might be Malicious based on GTI file reputation seen on a small number of systems

**Default State:** Evaluate

**Changes in this release:** Updated algorithm to improve detection effectiveness

**Affected Products:**

- ✓ Cloud-AV
- ✓ WSS 15.1

**Rules That Changed Exposure or Security Posture:**

None.

**Notes:**

**None.**