



## Threat Intelligence Exchange Rule Content Update 883 Release Notes: 2018-3-15

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

### New Rules

None

### Updated Rules

**Rule 324** – Prevent mshta from launching suspicious process

**Description:** Attempts to prevent Prevent mshta from launching suspicious process

**Default State:** Evaluate

**Changes in this release:** Improve detection effectiveness

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions

**Rule 322** – Prevent mshta from being launched by any process for all rule group assignments

**Description:** Prevent mshta from being launched by default on all rule group systems

**Default State:** On

**Changes in this release:** Improve in Detection Effectiveness

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions



**Rule 243** – Identify and block suspicious process executions

**Description:** This rule identifies and blocks suspicious execution of a process in an application by giving dirty reputation

**Default State:** Evaluate

**Changes in this release:** Improve product performance

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ WSS 15.x, 16.x versions

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

None

**Notes:**

For more information refer the [KB82925](#).