Threat Intelligence Exchange and ATP Rule Content Update 886

Release Notes: 2018-3-26

Below is the new/modified rule information for McAfee Threat Intelligence Exchange And ATP Rule content.

New Rules

None

Updated Rules

Rule 304 – Identify suspicious payloads targeting Browser related applications

Description: Identify suspicious payloads including unknown binaries targeting Browser applications like Firefox, Chrome, Edge and Others

Default State: Evaluate

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 303 – Identify highly suspicious payloads targeting Browser related applications

Description: Identify highly suspicious payloads including unknown binaries targeting Browser applications like Firefox, Chrome, Edge and Others

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
- ✓ Threat Intelligence Exchange for Virus Scan

Rule 239 – Identify suspicious command parameter execution

Description: This rule identifies suspicious execution of an application through execution parameters

Default State: On

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
- ✓ Threat Intelligence Exchange for Virus Scan

Rule 126 – Identify trusted signed applications

Description: This rule identifies files that are signed and have a valid non self-signed certificate. File location is considered along with environmental attributes such as Start menu entry.

Default State: Mandatory

Changes in this release: Support for CaseSensitivity feature of WindowsOS

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ WSS 15.x, 16.x versions
- ✓ Threat Intelligence Exchange for Virus Scan

Rules That Changed Exposure or Security Posture:

None

Notes:

For more information refer the KB82925.