Threat Intelligence Exchange Rule Content Update 745

Release Notes: 2018-05-17

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

New Rules

None.

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: Improve performance in offline mode

Affected Products:

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

Rule 126 – Identify trusted signed applications

Description: Identifies files that are signed and located in paths commonly used for installing programs. They also may have a Start menu entry

Default State: Mandatory

Changes in this release: Improve performance in offline mode

Affected Products:

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

Rule 127 – Identify trusted Help resource libraries

Description: Identifies signed resource libraries that are used by trusted software

Default State: Mandatory

Changes in this release: Improve performance in offline mode

Affected Products:

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

Rule 132 – Identify trusted signed files

Description: Identifies files that are signed and trusted, and whose certificate reputation is trusted

Default State: Mandatory

Changes in this release: Improve performance in offline mode

Affected Products:

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

Rule 151 – Identify web installers

Description: Identifies web installers that are signed and whose certificate is not distrusted. It also identifies the company, product, and version

Default State: Mandatory

Changes in this release: Improve performance in offline mode

Affected Products:

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

Rule 152 – Identify safe files extracted by Windows Installer

Description: Identifies safe files extracted by Windows Installer installer based on the actor process, certificate and cloud reputation

Default State: Evaluate

Changes in this release: Improve performance in offline mode

Affected Products:

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

Rule 239 – Identify suspicious command parameter execution

Description: Identifies the suspicious execution of an application through command line parameters

Default State: On

Changes in this release: Improve Detection Effectiveness

Affected Products:

✓ Endpoint Security 10.5.x version

Rule 243 – Identify and block suspicious process executions

Description: Identifies and blocks the suspicious execution of a process in an application

Default State: Evaluate

Changes in this release: Improve Detection Effectiveness

Affected Products:

✓ Endpoint Security 10.5.x version

Rules That Changed Exposure or Security Posture:

None.

Notes:

None.