



Threat Intelligence Exchange Rule Content Update 729

Release Notes: 2018-03-31

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

New Rules

None.

Updated Rules

None.

Rules That Changed Exposure or Security Posture:

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: On

Changes in this release: Exposure changed from Mandatory to On to allow user control

Affected Products:

- ✓ Endpoint Security 10.5.3 version
- ✓ 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: On

Changes in this release: Exposure changed from Mandatory to On to allow user control

Affected Products:

- ✓ Endpoint Security 10.5.3 version



- ✓ 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

Notes:

None.