Threat Intelligence Exchange Rule Content Update 560

Release Notes: 2016-10-20

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

New Rules

None.

Updated Rules

Rule 128 – Identify trusted help resource libraries

Description:

Identifies signed resource libraries that are used by trusted software. These libraries are generally used as part of Help documentation

Default State: Mandatory

Changes in this release:

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

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 detection effectiveness**

Rule 153 – Identify files that ATD does not report as suspicious

Description:
Identifies files that Advanced Threat Defense does not report as suspicious

Default State: Evaluate

Changes in this release:

- **Updated algorithm to improve detection effectiveness**

Rules That Changed Exposure or Security Posture:

None

Notes:

None.