Threat Intelligence Exchange Rule Content Update 695

Release Notes: 2017-08-22

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

New Rules

Rule 136 – Identify unsigned NativeImage Files that Might Be Trusted

Description: Detects pre compiled binary files that Might Be Trusted that have been installed into the NativeImages folder and do not contain suspicious attributes

Default State: Evaluate

Changes in this release: New Rule to identify trusted native image files

Affected Products:

- ✓ 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

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. The certificate reputation must be Known Malicious, Known Trusted, Most Likely Malicious, or Most Likely Trusted

Default State: Mandatory

Changes in this release: Add logic to improve performance

Affected Products:

- ✓ 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

Rules That Changed Exposure or Security Posture:

Rule 137 – Identify unsigned DOTNet assemblies that Might Be Trusted

Description: Detects DOTNet assemblies that are not signed with a known trusted certificate. These files are often low prevalence and may be unique to a system

Changed State: On

Affected Products:

- ✓ 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 239 – Identify suspicious command parameter execution

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

Default State: Off

Changes in this release: Changes in logic to improve detection effectiveness in progress

Affected Products:

- ✓ Endpoint Security 10.2 and 10.5.x versions
- ✓ WSS 15.x, 16.x versions

Notes:

None.