

Threat Intelligence Exchange Rule Content Update 653

Release Notes: 2017-04-25

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

New Rules

Rule 51 – Identify files marked as trusted installers by the Trust Scanner

Description: Identifies files that are marked as trusted by the Trust scanner which is based off the dat file

Default State: Mandatory

Changes in this release: New rule to identify files that are marked as trusted installer files by Trust scanner

Affected Products:

- ✓ Endpoint Security 10.5.1 version

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.

Default State: Evaluate

Changes in this release: New rule to detect files that Might Be Trusted that have been installed into the global assembly cache folders and do not contain suspicious attributes.

Affected Products:

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

Updated Rules

Rule 10 – Identify that a file is the main component of a trusted installer using the file's attributes, certificate reputation, and file reputation

Description: Determines whether a file is a trusted installer based on the file's attributes, filename, and the GTI or Enterprise certificate and file reputation

Default State: Mandatory

Changes in this release: Optimized logic and improve detection effectiveness

Affected Products:

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

Rule 129 – Identify trusted signed utility applications

Description: Identifies utility applications that are signed and the certificate is not distrusted. These files do not launch on startup and have characteristics that suggest they are utility programs

Default State: Mandatory

Changes in this release: Updated algorithm to improve detection effectiveness

Affected Products:

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

Rule 130 - Identify trusted signed drivers

Description: Identifies device drivers that are signed and installed on the local system

Default State: Mandatory

Changes in this release: Updated algorithm to improve detection effectiveness

Affected Products:

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

Rule 131 - Identify trusted signed Digital Rights Management (DRM) libraries

Description: Identifies signed trusted Digital Rights Management libraries used by Windows

Default State: Mandatory

Changes in this release: Updated algorithm to improve detection effectiveness

Affected Products:

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

Rules That Changed Exposure or Security Posture:

Rule 11 – Identify that the file is the main component of a trusted installer using the file's certificate reputation

Description: Determines whether a file is a trusted installer based on the file name and the GTI or Enterprise certificate reputation used to sign the file

Changed State: Removed the rule

Changes in this release: The algorithm for Trusted Installer (Rule 10) was updated to include Certificate based trust, making this rule (Rule11) obsolete

Affected Products:

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

Rule 57 – Use GTI file reputation to identify files that Might be Trusted or Might be Malicious

Description: Determines files which Might be Trusted or Might be Malicious based on GTI file reputation

Changed State: On

Changes in this release: The algorithm was changed to reduce false



Affected Products:

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

Notes:

None.