

Threat Intelligence Exchange Rule Content Update 468

Release Notes: 2016-06-23

Below is the new/modified rule information for McAfee Threat Intelligence Exchange 1.0

New Rules

Rule 138 - Identify trusted unsigned Microsoft DOTNet assemblies

Description:

This rule detects Microsoft-provided files that have a CLR code (DOTNet), have been installed into the global assembly cache folders, and do not contain suspicious attributes. The files may or may not be found on multiple machines within the enterprise, which could include just-in-time compiled assemblies.

Default State: Evaluate

Updated Rules

None.

Rules That Changed Exposure or Security Posture:

None.

Notes:

This package adds support for TIE Module for ENS 10.2.