



McAfee TIE and ATP Rule Content Update - 956

Below is the new/modified rule information for McAfee Threat Intelligence Exchange and ATP Rule content update

New Rules

Rule 260 – Detect AMSI bypass techniques

Description: This rule is designed to prevent different techniques used by bad guys to bypass Antimalware Scan Interface(AMSI)

Default State: Evaluate

Changes in this release: New rule to detect situations where AMSI detections are tried to be bypassed

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions

Updated Rules

None

Rules That Changed Exposure or Security Posture:

None

Notes:

For more information refer the [KB82925](#).