McAfee Exploit Prevention Linux Content 00206

Release Notes | 2021-09-21

Content package version for –

McAfee Endpoint Security Exploit Prevention for Linux: 10.7.0.00206[1]

[1] - Applicable on McAfee Endpoint Security for Linux for versions 10.7.2 and later

New Linux Signatures	Minimum Supported Product version Endpoint Security Exploit Prevention for Linux
Signature 50026: *T1547.013 - Boot or Logon Autostart Execution: XDG Autostart Entries* *Description:* - *This event indicates that the XDG autostart entries are created or modified in the system. As part of persistence, an adversary may execute malicious payload by creating or modifying XDG autostart entries.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.* *This is a monitoring/telemetry signature and customers are advised to enable this signature on basis of their requirement.*	*10.7.2*
Signature 50027: *Possible DarkRadiation Ransomware Infection Detected* *Description:* - *This event indicates a possible DarkRadiation Ransomware Infection. The malware targets Red Hat and Debian based Linux distribution to install Ransomware and uses Telegram API for C2 communication. DarkRadiation also contains a worm component that has the ability to infect additional computers on internal networks via SSH.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.2*
Signature 50028: *Possible FaceFish Malware Infection Detected* *Description:* - *This event indicates a possible FaceFish Malware Infection. The malware performs Dropper, Rootkit, Backdoor and Information Stealer activities. Rootkit activities is performed via LD_PRELOAD feature and its backdoor*	*10.7.2*

capabilities allows it to collect system information, credentials, execute arbitrary commands and provides shell access to the victim machine. - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	
Signature 50029: *TeamTNT: Suspicious Credential Stealing Activity Detected* *Description:* - *This event indicates TeamTNT Threat group enumerating the linux instances for stealing credentials and/or perform cryptocurrency mining activities. The malware attempts to enumerate AWS and GCP credentials as well as application credentials from the Linux instances.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.2*

Updated Linux Signatures	**Minimum Supported Product version** **Endpoint Security Exploit Prevention for Linux**
Signature Description modification: *The signature description has been modified for the below signatures*	
Signature 50018: *T1070.003 - Indicator Removal on Host: Clear Command History*	*10.7.2*
Signature 50019: *T1543.002 - Create or Modify System Process: Systemd Service*	*10.7.2*
Signature 50020: *T1053.006 - Scheduled Task/Job: Systemd Timers*	*10.7.2*
Signature 50021: *T1098.004 - Account Manipulation: SSH Authorized Keys*	*10.7.2*
Signature 50022: *TeamTNT: Suspicious Cryptocurrency Mining Activity Detected*	*10.7.2*
Bugfix: *The below signature has been modified to enhance the protection - added coverage for additional malware families*	
Signature 50023: *Possible Crypto-Currency Miner Activities Detected*	*10.7.2*

NOTE: Refer to the KB for the default Reaction-type associated with Signature severity level for all supported Product versions:
https://kc.mcafee.com/corporate/index?page=content&id=KB90369

How to Update

Please find below the KB article reference on how to update the content for following products:

1. McAfee Endpoint Security Exploit Prevention:
https://kc.mcafee.com/corporate/index?page=content&id=KB92136