McAfee Exploit Prevention Linux Content 00079

Release Notes | 2020-11-03

Content package version for –

McAfee Endpoint Security Exploit Prevention for Linux: 10.7.0.00079[1]

[1] - Applicable only on McAfee Endpoint Security for Linux for version 10.7.2

New Linux Signatures	Minimum Supported Product version Endpoint Security Exploit Prevention for Linux
Signature 50001: *Possible WatchBog Malware Infection Detected* *Description:* - *This event indicates a possible WatchBog Malware Infection. The malware targets Linux servers running a range of vulnerable software such as Jira (CVE-2019-11581), Exim (CVE-2019-10149), Solr (CVE-2019-0192), Jenkins (CVE-2018-1000861), Nexus Repository Manager 3 (CVE-2019-7238) to mine crypto-currency.* - *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 50002: *Possible Skidmap Malware Infection Detected* *Description:* - *This event indicates a possible Skidmap Malware Infection. The malware targets Linux servers running a range of vulnerable software to mine crypto-currency. Skidmap also contains rootkit components to hide its file, process and network artifacts.* - *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 50003: *Possible Xbash Ransomware Infection Detected* *Description :* - *This event indicates a possible Xbash Ransomware Infection. The malware targets Windows and Linux servers running a range of vulnerable software to turn the computer into a botnet, mine crypto-currency, and install ransomware. Xbash also contains a worm component that has the ability to scan and infect additional computers on internal networks.* - *The signature is disabled by default.*	*10.7.2*

Note: Customer can change the level/reaction-type of this signature based on their requirement	
Signature 50004: *Possible EvilGnome Backdoor Infection Detected* *Description:* - *This event indicates a possible EvilGnome Backdoor Infection. Possible Threat actor associated with the malware would be the Gamaredon Group. The malware targets Linux servers running a range of Vulnerable software to perform backdoor and information stealing activities.* - *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 50005: *Possible KORKERDS Malware Infection Detected* *Description :* - *This event indicates a possible KORKERDS Malware Infection. The malware targets Linux servers via malicious third-party plugins/software to mine crypto-currency on the victim machine.* - *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 50006: *Rocke Group Malware Detected* *Description :* - *This event indicates a possible Malware Infection associated with the Threat Actor group Rocke. This malware targets Linux servers running a range of vulnerable software such as Apache Struts 2, Oracle WebLogic (CVE-2017-10271) and Adobe ColdFusion (CVE-2016-3088) to mine crypto-currency.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement*	*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 (Windows and Linux):
https://kc.mcafee.com/corporate/index?page=content&id=KB92136