McAfee Exploit Prevention Linux Content 00184

Release Notes | 2020-06-15

Content package version for –

McAfee Endpoint Security Exploit Prevention for Linux: 10.7.0.00184[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 50014: *Possible Kinsing Malware Infection Detected* *Description:* - *This event indicates a possible Kinsing Malware Infection. The malware targets Linux servers running a range of vulnerable software such as Liferay (CVE-2020-7961), SaltStack (CVE-2020-11651, CVE-2020-11652) and Exposed Docker Daemon APIs to mine crypto-currencies.* - *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 50015: *Possible Kinsing Malware Infection Detected II* *Description:* - *This event indicates a possible Kinsing Malware Infection. The malware targets Linux servers running a range of vulnerable software such as Liferay (CVE-2020-7961), SaltStack (CVE-2020-11651, CVE-2020-11652) and Exposed Docker Daemon APIs to mine crypto-currencies.* - *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 50016: *Possible RedXor Backdoor Infection Detected* *Description:* - *This event indicates a possible RedXor Backdoor Infection. RedXor malware uses XoR Scheme to encode malware's network data and establishes communication with the C2 Server to upload, download, create, write, delete contents remotely on the compromised machine.* - *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 50017: *Possible WatchDog Malware Infection Detected* *Description:* - *This event indicates a possible WatchDog Malware Infection. The malware targets Linux servers running a range of vulnerable software such as Elasticsearch (CVE-2015-1427, CVE-2014-3120), Apache Hadoop, Spring Data Commons (CVE-2018-1273), ThinkPHP, Oracle WebLogic Server (CVE-2017-10271) to mine crypto-currencies.* - *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 50018: *T1070.003 - Indicator Removal on Host: Clear Command History* *Description :* - *This event indicates when bash history file is deleted. As part of Defense Evasion, an adversary may delete the bash history file in a compromised account to conceal the commands executed during an intrusion.* - *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 fine tune the signature based on the applications used in their environment or to disable the signature in case of false positives.*	*10.7.2*
Signature 50019: *T1543.002 - Create or Modify System Process: Systemd Service* *Description:* - *This event indicates when systemd services were created or modified in the system. As part of persistence, an adversary may execute malicious payload by creating or modifying systemd services.* - *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 fine tune the signature based on the applications used in their environment or to disable the signature in case of false positives.*	*10.7.2*
Signature 50020: *T1053.006 - Scheduled Task/Job: Systemd Timers* *Description:* - *This event indicates when systemd timers were created or modified in the system. As part of persistence, an adversary may execute malicious payload by creating or modifying systemd timers.* - *The signature is disabled by default.*	*10.7.2*

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 fine tune the signature based on the applications used in their environment or to disable the signature in case of false positives.*	
Signature 50021: *T1098.004 - Account Manipulation: SSH Authorized Keys* *Description:* - *This event indicates when new SSH public key has been added or modified in the system. As part of persistence, an adversary may modify the SSH authorized_keys 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.* *This is a monitoring/telemetry signature and customers are advised to fine tune the signature based on the applications used in their environment or to disable the signature in case of false positives.*	*10.7.2*
Signature 50022: *TeamTNT Group Malware Detected* *Description:* - *This event indicates cryptocurrency miner activities associated with the TeamTNT Threat group. The malware targets Linux servers having Exposed Docker Daemon APIs to mine crypto-currencies.* - *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 50023: *Possible Crypto-Currency Miner Activities Detected* *Description:* - *This event indicates cryptocurrency miner activities associated with multiple malware families - RootTmpBash, Xmrig miner, dbusex and carbine loader.* - *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 50024: *Possible Crypto-Currency Miner Activities Detected II* *Description:* - *This event indicates suspicious cryptocurrency miner activities associated with multiple malware families - Moneroocean xmrig miner, cpumon, systemd repair miner.* - *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 50025: *Possible Jakiro Backdoor Infection Detected* *Description:*	*10.7.2*

- *This event indicates a possible Jakiro Backdoor Infection. Jakiro can collect system information, steal sensitive information, query/deliver/delete - file/plugin/directory based on the instruction from C2 server.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	

Updated Linux Signatures	**Minimum Supported Product version** **Endpoint Security Exploit Prevention for Linux**
Signature Description modification: *The signature description for the below signatures have been modified for grammatical corrections*	
Signature 50001: *Possible WatchBog Malware Infection Detected*	*10.7.2*
Signature 50002: *Possible Skidmap Malware Infection Detected*	*10.7.2*
Signature 50003: *Possible Xbash Ransomware Infection Detected*	*10.7.2*
Signature 50005: *Possible KORKERDS Malware Infection Detected*	*10.7.2*
Signature 50006: *Rocke Group Malware 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