Trellix Exploit Prevention Content 12408

Release Notes | 2022-09-13

Content package version for –

Trellix Endpoint Security Exploit Prevention: 10.6.0.12408[1]

Trellix Host Intrusion Prevention: 8.0.0.12408[2]

[1] - Applicable on all versions of Trellix Endpoint Security Exploit Prevention including version 10.7.x

[2] - Applicable on all versions of Trellix Host Intrusion Prevention content including Host IPS 8.0 Patch 16.

IMPORTANT NOTE – ACTION MAY BE REQUIRED: This release of ***Endpoint Security Exploit Prevention content*** contains new signing certificates as part of the continued Trellix rebranding efforts. These certificates are signed by new third-party root and intermediate certificate authorities. If your organization manually manages deployment of third-party root and intermediate certificate authority certificates to your devices, you will need to deploy the appropriate third-party and intermediate certificates to your devices before using this software. Failing to do so could impact or break the functionality of this software. This is an action your organization needs to take if you do not leverage automatic root certificate updating options like the one available for Microsoft Windows Operating Systems.

Please see KB95499 for certificate details and more information about the Trellix rebranding efforts.

IMPORTANT:

1. Exploit Prevention content binaries are signed with New Musarubra certificates replacing old McAfee certificates. Trellix V3 Virus Definition Updates (DATs) version 4826 (released on June 10, 2022) or later versions is a mandatory prerequisite for this Exploit prevention content update on Trellix Endpoint Security version 10.6.x and 10.7.x.

   For more information, see KB95907 - Exploit Prevention engine stops functioning after you update to content version 12336 or later

   For customers with extended support for Host IPS product, it is recommended to have the latest Host IPS 8.0 Patch 16 extension.

New Windows Signatures	Minimum Supported Product version	
	Endpoint Security Exploit Prevention	Host Intrusion Prevention
Signature 6234: *Excel 4 Macro Executing Shellcode in Memory* *Description:* *- This event indicates an attempt to inject shellcode and execute it using Excel 4 macro.* *- The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement*	*10.6.0*	*Not Applicable*

Signature 6235: *WMIC Abuse by Microsoft Excel* *Description:* *- This event indicates the use of Excel 4 macro by malware to abuse Windows Management Instrumentation Command line (WMIC). Such behaviour is seen by malwares like Ursnif (aka Gozi, Dreambot, ISFB). This is a banking trojan that collects victim's system activity, keystrokes and network/browser activity.* *- The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement*	*10.6.0*	*Not Applicable*
Signature 6236: *Cobalt Strike Named Pipe Communication Detected* *Description:* *- This event indicates a named pipe communication by cobalt strike. A named pipe is a way of communicating between two processes. Cobalt Strike is a commercial adversary simulation software that is marketed to red teams but is also stolen and actively used by a wide range of threat actors from ransomware operators to espionage-focused Advanced Persistent Threats (APTs).* *- The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement*	*10.6.0*	*Not Applicable*

Updated Windows Signatures	Minimum Supported Product version	
	Endpoint Security Exploit Prevention	Host Intrusion Prevention
Additional Coverage: *GBOP coverage has been updated for process spoolsv.exe*	*10.6.0*	*8.0.0*
Bug Fix: *Trusted Application list has been modified to resolve syntax issues.*	*Not Applicable*	*8.0.0*

Existing Coverage for New Vulnerabilities	Minimum Supported Product version	
	Endpoint Security Exploit Prevention	Host Intrusion Prevention
Coverage by GPEP: *Generic Privilege Escalation (Signature 6052) is expected to cover the below vulnerabilities:* *- CVE-2022- 34729*	*10.6.0*	*8.0.0*

NOTE:

1. For more information on the deprecation of applicable signatures, see: KB94952 - List of obsolete signatures deprecated from Exploit Prevention and Host Intrusion Prevention as of October 2021 content.
2. For more information on the default Reaction-type associated with Signature severity levels for all supported product versions, see: KB90369 – Exploit Prevention actions based on signature severity level.
3. Trellix maintains additional Expert Rules for use in Trellix Endpoint Security's Exploit Prevention policy that can provide increased coverage for more specific requirements. For more information, see Trellix ExpertRules GitHub Repository.

   IMPORTANT: Trellix recommends testing Expert Rules in a non-production test environment to ensure rule integrity, and to prevent conflicts with unique environment configurations. Customers should exercise caution when deploying Expert Rules in their environment.

HOW TO UPDATE

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

1. Trellix Endpoint Security Exploit Prevention:

KB92136 – Exploit Prevention signature content updates and remediation rollback version for troubleshooting.

2. Trellix Host Intrusion Prevention:

KB53092 – Information about Host IPS signature content updates