Trellix Exploit Prevention Content 12336

Release Notes | 2022-08-09

Content package version for –

Trellix Endpoint Security Exploit Prevention: 10.6.0.12336[1]

Trellix Host Intrusion Prevention: 8.0.0.12336[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 6228: *T1457 – LNK File Added To Startup Folder* *Description:* *- This event indicates an attempt to add LNK file to startup folder by suspicious process. An LNK file is a Windows shortcut, which points to and is used to open another file, folder, or application. This behaviour is exhibited by Malware Yellow Cockatoo to gain persistence.* *- 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*

This is a monitoring type of rule and recommended be enabled at Report only mode.		
Signature 6229: *MSDT Remote Code Execution Vulnerability Detected* *Description:* *- This event indicates an attempt to abuse remote code execution vulnerability in Microsoft Support Diagnostic Tool aka MSDT. This is a legitimate Microsoft tool part of microsoft's troubleshooting pack which can be used to gain system control by unauthenticated attacker. This vulnerability abuse is popularly being referred to as follina.* *- 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 type of rule and recommended be enabled at Report only mode*	*10.6.0*	*Not Applicable*
Signature 6231: *Coinminer Activity Detected* *Description:* *- This event indicates suspicious activity similar to coin miners. Such malwares use computing power to generate Bitcoins and can make the system run slower than usual.* *- 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 6232: *Gootkit Trojan Detected* *Description:* *- This event indicates abuse of cscript and wscript to enable surreptitious loading of Gootkit loader. Gootkit is a banking trojan that can deliver additional payloads, siphon data from victims, and stealthily persist in a compromised environment.* *- 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 6233: *ADSelfService Plus Authentication ByPass Attempt* *Description:* *- This event indicates adversarial use of Java utility Keytool to execute a malicious web shell. Keytool is a certificate management utility included with Java.* *- 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
False Positive Reduction: *The below signature has been modified to reduce the false positives*		

- **Signature 2226:** *Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution*	*10.6.0*	*NA*

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