Trellix Exploit Prevention Content 12194

Release Notes | 2022-06-14

Content package version for –

Trellix Endpoint Security Exploit Prevention: 10.6.0.12194[1]

Trellix Host Intrusion Prevention: 8.0.0.12194[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:

1. Trellix V3 Virus Definition Updates (DATs) version 3786 or above is a mandatory prerequisite for this Exploit prevention content update on Trellix Endpoint Security version 10.6.x only.

   For more information, see KB91867 - Exploit Prevention engine stops functioning after you update to content version 9528 or later.

2. 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	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Signature 6226: *PowerShell Command Restriction - UnquotedService* *Description:* *- This event indicates an attempt to execute Powershell Core with UnquotedService parameter.* *- 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.*	*Not Applicable*	*10.6.0*

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
False Positive Reduction: *The below signature has been modified to reduce the false positives*		
- **Signature 6131:** *T1047 - Weaponized OLE object infection via WMI*	*Not Applicable*	*10.6.0*
Extended Coverage: *The below signatures are modified to cover an additional process "certutil.exe"*		

- **Signature 6195:** *IIS worker process trying to execute unwanted program*	*Not Applicable*	*10.6.0*

Other Changes	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Bugfix*: Inclusion of New Musarubra Certificates* *Both Endpoint Security Exploit Prevention Content and Host Intrusion Prevention Content have been modified to support the new Musarubra Certificate signer. Trusted application list has been modified to support the new Musarubra Certificate Signer.*	*8.0.0 (Patch 16)*	*10.6.0*

Deprecated Windows Signatures

The following signatures have been deprecated from Endpoint Security Exploit Prevention and Host IPS products as they were identified as obsolete based on the vulnerability and the platforms it supports.

Note:
There's no intervention needed from customers. Also, this change doesn't affect custom signature policies configured for Exploit Prevention in ePolicy Orchestrator.

Signature ID	Signature Name	CVE Reference	Minimum Supported Product version	
			Host Intrusion Prevention	Endpoint Security Exploit Prevention
2202	*Vulnerabilities in GDI Could Allow Remote Code Execution (CVE-2008-2249)*	*CVE-2008-2249*	*8.0.0*	*10.6.0*
2240	*Windows Metafile Denial of Service Vulnerability (2)*	*NA*	*8.0.0*	*10.6.0*
2819	*Windows Enumerate File Vulnerability*	*CVE-2012-4774*	*8.0.0*	*10.6.0*
3769	*Windows Metafile Denial of Service Vulnerability*	*CVE-2006-4071*	*8.0.0*	*10.6.0*
3948	*Windows Metafile Remote Code Execution Vulnerability*	*CVE-2008-3014*	*8.0.0*	*10.6.0*

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