Erstellen einer erweiterten Liste benutzerdefinierter Erkennungsoptionen in Cisco Secure Endpoint

Inhalt

Einleitung Hintergrundinformationen Voraussetzungen Anforderungen Verwendete Komponenten Erweiterte benutzerdefinierte Erkennungsliste erstellen Zugehörige Informationen

Einleitung

In diesem Dokument werden die Schritte zum Erstellen einer erweiterten benutzerdefinierten Erkennung (ACD) in Cisco Secure Endpoint beschrieben.

Hintergrundinformationen

TALOS Intelligence veröffentlichte am 14. Januar 2020 als Antwort auf die dienstlichen Sicherheitslücken von Microsoft Patch einen BLOG.

Aktualisiert am 15. Januar: ACD-Signatur für AMP hinzugefügt, die zum Erkennen der Ausnutzung von CVE-2020-0601 verwendet werden kann, indem Zertifikate getauscht werden, die als Microsoft ECC Code Signing Certificate Authority maskiert werden: https://blog.talosintelligence.com/2020/01/microsoft-patch-tuesday-jan-2020.html.

Die Signatur der Datei im TALOS-BLOG, die in der ACD verwendet werden soll:

- Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D020130
- https://alln-extcloud-storage.cisco.com/blogs/1/2020/01/CVE-2020-0601.txt

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-

Versionen:

- Cisco Secure Endpoint Cloud Portal
- ACD
- TALOS-Blog

Die Informationen in diesem Dokument wurden von Geräten in einer bestimmten Laborumgebung erstellt. Alle verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Erweiterte benutzerdefinierte Erkennungsliste erstellen

Nun erstellen wir die ACD, um sie abzugleichen.

Schritt 1: Navigieren Sie zu Secure Endpoint Portal > Outbreak Control > Advanced Custom Detection wie im Bild gezeigt.

Outbreak Control Mana
CUSTOM DETECTIONS
Simple
Advanced പ്രിസ
Android
APPLICATION CONTROL
Blocked Applications
Allowed Applications
NETWORK
IP Block & Allow Lists
ENDPOINT IOC
Initiate Scan
Installed Endpoint IOCs
Scan Summary

Schritt 2: Beginnen Sie mit einem Namen für den Signaturensatz CVE-2020-0601, wie im Bild gezeigt.

Custom Detections - Advanced				
		Create Signature Set		
Name	I	Save		

Schritt 3: **Bearbeiten** Sie anschließend diesen neuen Signatursatz, und **fügen Sie die Signatur** hinzu. Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D020130.

Custom Detections - Advanced

	Create Signature Set	CVE-2020-0601	Update Name	
CVE-2020-0601 Created by Mustafa Shukur • 2020-01-22 12:19:38 CST Used in policies: Used in groups:		Created by Mustafa Shukur • 2020-01-22 12:19:38 CST Add Signature Build Database From Signature Set ndb: Win.Exploit.CVE_2020_0601.UNOFFICIAL		
O View Changes	🛓 Download 🛛 🖉 Edit 🔹 Delete			

O View All Changes

Schritt 4: Wählen Sie Datenbank aus Signatursatz erstellen, und die Datenbank wurde erstellt.

Schritt 5: Wenden Sie den neuen Signatursatz auf eine Richtlinie an, und klicken Sie auf **Bearbeiten> Outbreak-Kontrolle > Benutzerdefinierte Erkennungen > Erweitert** wie im Bild gezeigt.

Modes and Engines	Custom Detections - Simple	None	~		
Exclusions 3 exclusion sets					
Proxy	Custom Detections - Advanced	CVE-2020-0601	~		
Outbreak Control		None CVE-2020-0601			
Product Updates	Application Control - Allowed	None	~		
Advanced Settings					
	Application Control - Blocked	None	~		
	Network - IP Block & Allow Lists	Clear Select Lists	×		
				Cancel	Save

Schritt 6: Speichern Sie die Richtlinie und Synchronisierung auf der Benutzeroberfläche des Connectors, wie im Bild gezeigt.



Schritt 7: Suchen Sie im Verzeichnis C:\Program Files\Cisco\AMP\ClamAV nach einem neuen Signaturordner, der an diesem Tag erstellt wurde, wie im Bild gezeigt.

<mark></mark> 0.101.4.71		1/22/2020	12:30 PM	File folder
	n			
📄 custom2522620200122121949.cud		1/22/2020 12:30 PM	CUD File	1 KB
daily.cvd	~	5/24/2019 12:37 PM	CVD File	11 KB
📄 freshclam.conf		1/22/2020 12:30 PM	CONF File	1 KB
👼 freshclam.exe		12/20/2019 11:26 AM	Application	122 KB
👼 freshclamwrap.exe		12/20/2019 11:26 AM	Application	65 KB

Zugehörige Informationen

- Der für den Test verwendete Build ist Windows 10 1909, der von der Sicherheitslücke im MSKB nicht betroffen ist; <u>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601</u>
- https://support.microsoft.com/en-us/help/4534273/windows-10-update-kb4534273
- Gilt für: Windows 10, Version 1809, Windows Server Version 1809, Windows Server 2019, alle Versionen
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>