Empfohlene Vorgehensweisen für die Planung einer Aktualisierung von sicherem Firewall-Inhalt

Problem

Unternehmen, die Firewall Threat Defense (FTD)-Geräte mit Firewall Management Center (FMC) verwalten, benötigen Beratung zu Best Practices für die Anwendung von Sicherheits- und Content-Updates. Insbesondere besteht Unsicherheit darüber, wie häufig verschiedene Aktualisierungstypen angewendet werden müssen, ob Updates geplant und nicht sofort angewendet werden können und welche betrieblichen Auswirkungen diese Updates haben. Die Frage stellt sich, da Cisco Content-Updates häufig, manchmal wöchentlich, veröffentlicht. Administratoren müssen wissen, ob diese sofort nach der Veröffentlichung angewendet werden müssen oder ob sie gemäß organisatorischer Wartungsfenster und Änderungsmanagementrichtlinien geplant werden können.

Umwelt

- Cisco Secure Firewall FirePOWER, alle Versionen
- FirePOWER Management Center, alle Versionen

Auflösung

Diese Tabelle zeigt den Zweck jedes Aktualisierungstyps in Firepower.

Aktualisierungstyp	Zweck	Hinweise
SRU/LSP	Aktualisierungen der Angriffsregeln (Snort 2 und Snort 3)	Beibehaltung der Regeln zur Identifizierung von/zum Schutz vor Sicherheitsrisiken

GeoDB	Standortdaten für IP-Adressen	Für geolokationsbasierte Datenverkehrsfilterung
VDB	Schwachstelleninformationen und Host-Fingerprints	Zur Schwachstellenbewertung und Risikoanalyse

Inhaltsupdates für die Cisco Secure Firewall sind in drei Kategorien eingeteilt, jede mit unterschiedlichen Veröffentlichungshäufigkeiten und empfohlenen Vorgehensweisen für die Zeitplanung. Diese Tabelle enthält die Best Practice-Planungsempfehlungen für jeden Aktualisierungstyp:

Aktualisierungstyp	Veröffentlichungshäufigkeit	Vorgeschlagener Zeitplan	Standard-FMC-Zeitplan	Navigationspfad (zu ändern)
SRU/LSP	Häufig	Täglich	Täglich	System > Inhaltsaktualisierungen > Regelaktualisierungen
GeoDB	~Wöchentlich	Wöchentlich	Wöchentlich	System > Inhaltsaktualisierungen > Standortaktualisierungen
VDB	~monatlich	Wöchentlich	Wöchentlich	System > Tools: Planung > Wöchentlicher Software-Download

Für optimale Sicherheitskonfigurationen und -status gilt es, diese Updates nach der Veröffentlichung durch Cisco anzuwenden. Einige dieser Aktualisierungsdateien können relativ groß sein, und Bandbreitenzuweisungen müssen berücksichtigt werden. Es wird empfohlen, die größeren Updates außerhalb der Hauptverkehrszeiten zu installieren, wenn Sie dasselbe Netzwerk verwenden.

SRU/LSP-Aktualisierungen (Intrusion Rules)

Snort Rule Updates (SRU) und Lightweight Security Packages (LSP) enthalten Regeln zur Erkennung von und zum Schutz vor Sicherheitsrisiken. Diese Updates müssen so häufig wie möglich angewendet werden, um Schutz vor neuen Bedrohungen zu gewährleisten.

So ändern Sie den SRU/LSP-Zeitplan: Navigieren Sie zu System > Content Updates > Rule Updates (System > Inhaltsaktualisierungen > Regelaktualisierungen) in der FMC-Schnittstelle, um die Zeit-, Datum- und Frequenzeinstellungen anzupassen.

SRU/LSP-Updates unterstützen die automatisierte Bereitstellung und können so geplant werden, dass die Bereitstellung automatisch nach dem Herunterladen und der Installation erfolgt.

GeoDB (Geolocation Database)-Updates

Aktualisierungen der Standortdatenbank stellen aktuelle geografische Standortdaten für IP-Adressen zur Verfügung und werden in der Regel wöchentlich veröffentlicht.

So ändern Sie den GeoDB-Zeitplan: Navigieren Sie zu System > Content Updates > Geolocation Updates in der FMC-Schnittstelle, um die Planungsparameter anzupassen.

GeoDB-Updates können für Download und Installation geplant werden. Die Bereitstellung auf verwalteten Geräten erfordert jedoch manuelles Push und kann nicht vollständig automatisiert werden, wie dies bei SRU/LSP-Updates der Fall ist.

VDB-Updates (Vulnerability Database)

Sicherheitslücken-Datenbank-Updates werden ungefähr monatlich veröffentlicht und werden als Software-Updates und nicht als Content-Updates verwaltet.

So ändern Sie den VDB-Zeitplan: Navigieren Sie zu System > Tools: Planen und Ändern der wöchentlichen Software-Download-Aufgabe, um die Download-Häufigkeit und den Zeitpunkt anzupassen.

VDB-Updates unterliegen Software-Updates und können nicht unabhängig bereitgestellt werden. Sie werden bei der Durchführung manueller Bereitstellungen berücksichtigt, bei denen alle ausstehenden Änderungen kompiliert werden.

Überlegungen zur Bereitstellung

Bei der Bereitstellung von Updates kompiliert das FMC alle ausstehenden Konfigurationsänderungen und kann mehrere Arten von Inhaltsaktualisierungen in einem Bereitstellungsvorgang einschließen. Einige Updates können einen kurzen Neustart des Snort-Service während der Bereitstellung verursachen, was bei der Planung von Updates während der Produktionszeiten berücksichtigt werden muss.

Unternehmen müssen Aktualisierungspläne mit ihren Änderungsmanagementrichtlinien abstimmen und Aktualisierungen während Wartungszeitfenstern in Betracht ziehen, wenn kurze Serviceunterbrechungen für ihre Betriebsumgebung von Bedeutung sind.

Ursache

Dies war eher eine Anforderung nach Konfiguration und Betriebsanleitung als eine technische Störung. Klärungsbedarf bestand aufgrund der Unsicherheit hinsichtlich der Aktualisierungsplanung, der Automatisierungsfunktionen und der betrieblichen Auswirkungen verschiedener Aktualisierungstypen in Cisco Secure Firewall-Umgebungen.

Verwandte Inhalte

- Cisco Secure Firewall Management Center Administration Guide, 7.6: Updates
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.