مصفوفة توافق نظام كشف التسلل

المحتويات

المقدمة

يقدم هذا المستند مصفوفة توافق الأجهزة/البرامج لأجهزة نظام منع التسلل (IPS) من Cisco (4210، 4215، 4220، 4230، 4235، 4240، 4250، 4255)، ووحدة خدمات أمان جهاز الأمان القابل للتكيف (SSM)، ووحدة الموجه، ووحدات نظام اكتشاف الاقتحام (IDSM-1، IDSM-2 Catalyst 6000). كما يوفر هذا المستند نظرة عامة على خيارات الإدارة. يتم توفير نظرة عامة مختصرة على كل تطبيق، بالإضافة إلى مصفوفة توافق الإصدار. الإصدارات المدرجة في كل مصفوفة توافق هي الإصدارات الوحيدة المدعومة.

كان نظام Cisco لمنع الاقتحام يعرف سابقا باسم نظام اكتشاف الاقتحام (IDS) أو NetRanger. تعرف أجهزة نظام منع الاقتحام من Cisco أيضا باسم أجهزة الاستشعار. ارجع إلى وثائق المنتج ذات الصلة وملاحظات الإصدار للحصول على مزيد من المعلومات.

ملاحظة: كن على دراية بعمود حالة المنتج في الجداول ضمن هذا المستند. يشير هذا العمود إلى إعلامات نهاية العمر (EoL)/نهاية البيع (EoS) ذات الصلة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- أجهزة نظام منع التسلل (IPS) من Cisco (4210، 4215، 4220، 4230، 4235، 4240، 4250، 4255)
- الوحدة النمطية لخدمات أمان أجهزة الأمان المعدلة (SSM)
- الوحدة النمطية للموجه Router Module
- وحدات نظام اكتشاف الاقتحام (IDSM-1، IDSM-2 Catalyst 6000)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

توافق أجهزة/برامج IPS

الجدول 1 - الأجهزة

جهاز	رقم الجزء	الأجهزة	الواجهات الاختيارية	الأجهزة الإضافية المتوفرة	إصدارات البرامج المتوافقة	حالة المنتج
IDS-4210	IDS-4210 IDS-4210-K9 IDS-4210-NFR	يتوفر محرك أقراص IDE مع CDROM لترقية البرامج واسترداد الصور.		IDS-4210-MEM-U= ذاكرة إضافية سعة 256 ميجابايت لعملاء SmartNet فقط للترقية إلى الإصدار 4.1 والإصدارات الأحد	3.1 إلى الحالي *	انتهاء البيع: 8 ديسمبر 2003 اليوم الأخير من الدعم: 8 ديسمبر 2008

					ث. يستطيع العملاء طلب شراء الذاكرة من خلال أداة ترقية المنتجات (للعملاء المسجلين فقط).	
IDS-4215	IDS-4215-K9 IDS-4215-4FE-K9	محرك أقراص ثابتة IDE وذاكرة فلاش مضغوطة. لا يتوفر أي محرك أقراص CDROM لأغراض ترقية البرامج واسترداد الصور.	IDS-4FE-INT=		4.1 إلى الحالي *	متداولي
IDS-4220	IDS-4220-E	يتوفر محرك أقراص IDE مع CDROM لترقية البرامج واسترداد الصور.		IDS-4220-MEM-U= ذاكرة إضافية سعة 256 ميجابايت لعملاء SmartNet	من 3.1 إلى 4.1	**انتهاء البيع:** 31 يوليو 2002 **اليوم الأخير من الدعم:** 31 يوليو 2007

				فقط للترقية إلى الإصدار 4.1 والإصدارات الأحدث. يستطيع العملاء طلب شراء الذاكرة من خلال أداة ترقية المنتجات (للعملاء المسجلين فقط).		
IDS-4230	IDS-4230-FE	يتوفر محرك أقراص IDE مع CDROM لترقية البرامج واسترداد الصور.			من 3.1 إلى 4.1	**انتهاء البيع:** 31 يوليو 2002 **اليوم الأخير من الدعم:** 31 يوليو 2007
IDS-4235	IDS-4235-K9	يتوفر محرك أقراص ثابتة SCSI مع CDROM لأغراض ترقية البرامج	IDS-4FE-INT=	IDS-PWR= وحدة إمداد الطاقة الاحتياطية	3.1 إلى الحالي *	**انتهاء البيع:** 31 مايو 2005 **اليوم الأخير**

		واسترداد الصور.		طية		[رمز الدعم: 31 مايو 2010](#)
IPS-4240	بروتوكول IPS-4240-K9 IPS-4240-DC-K9 (وحدة التحكم في الشبكة (DC) التي يتم تشغيلها، متوافقة مع معيار NEBS فقط)	ذاكرة فلاش مضغوطة. لا يتوفر أي محرك أقراص CDROM لأغراض ترقية البرامج واسترداد الصور.			4.1.4 إلى الحالي *	متداول
IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	يتوفر محرك أقراص ثابتة SCSI مع CDROM لأغراض ترقية البرامج واسترداد الصور.	IDS-4FE-int= IDS-4250-SX-INT= IDS-xl-=INT	IDS-PW=R محرك الأقراص الثابتة الاحتياطي IDS-SCSI= وحدة إمداد الطاقة الاحتياطية	3.1 إلى الحالي *	[نهاية البيع فقط لنسخة Tx:31 مايو 2005 اليوم الأخير من دعم TX: 31 مايو 2010](#) لا يتأثر النظا

						مان الآخر ان لمعر ف 425 0 Ids) 425 0) بإعلا ن EoL هذا.
الطرا ز IPS-425 5	الطراز IPS-4255-K9	ذاكرة فلاش مضغوطة. لا يتوفر أي محرك أقراص CDROM لأغراض ترقية البرامج واسترداد الصور.			4.1.4 إلى الحالي *	متداو لي

الجدول 2 - الوحدات النمطية

وحدة	رقم الجزء	الأجهزة	الواجهات الاختيارية	الأجهزة الإضافية المتوفرة	إصدارات البرامج المتوافقة	حالة المنتج
SSM	ASA-SSM-AIP-10-K9 (وحدة خدمة أمان ASA AIP Security Service Module-10) ASA-SSM-	ذاكرة فلاش مضغوطة. لا يتوفر أي محرك أقراص CDROM لأغراض ترقية البرامج واسترداد			5.0 إلى الحالي *	متداول ي

	AIP-20-K9 (وحدة خدمة أمان ASA AIP Security Service Module (e-20	الصور.				
الوحدة النمطية للموجه Router Module	NM-CIDS-K9 NM-CIDS-=K9 (جزء # RMA فقط)	ذاكرة فلاش مضغوطة. لا يتوفر أي محرك أقراص CDROM لأغراض ترقية البرامج واسترداد الصور.			برنامج IOS® الإصدار 12.2(15)ZJ من Cisco أو إصدار أحدث من برنامج Cisco IOS الإصدار 12.3(4)T أو معرفات أحدث الإصدار 4.1 إلى الحالي *	متداول
آي دي إس إم-1	WS-X6381-IDS WS-X6381=-IDS (جزء # RMA فقط)	محرك الأقراص الصلبة IDE. لا يتوفر أي محرك أقراص مضغوطة CD ROM لأغراض ترقية البرامج أو إستردا			من 2.5 إلى 3.0	**انتهاء البيع: 20 أبريل 2003 اليوم الأخير من الدعم: 20 أبريل 2008**

		د الصور.				
آي دي إس إم-2	WS-SVC-IDS2-BUN-K9 WS-SVC-IDS2BUNK9 = (جزء # RMA فقط)	محرك أقراص ثابتة IDE وذاكرة فلاش مضغوطة. لا يتوفر أي محرك أقراص CDROM لأغراض ترقية البرامج واسترداد الصور.		4.0 إلى الحالي *	متداول ي

ملاحظة: أحدث إصدار من البرامج المتاحة وقت نشر هذا المستند هو 5.1. إذا كنت بحاجة إلى إصدار برنامج أحدث من 5.1، فتحقق من الوثائق الخاصة بهذا الإصدار من الرمز لضمان التوافق.

خيارات الإدارة والتكوينات

يمكنك إدارة أجهزة إستشعار IPS وتكوينها عبر واجهة سطر الأوامر، أو عبر إحدى أدوات التكوين أو الإدارة المدرجة في هذه الأقسام.

مركز إدارة CiscoWorks لأجهزة إستشعار IPS (IPS MC)

يعد مركز إدارة CiscoWorks لأجهزة إستشعار IPS أداة مزودة ببنية قابلة للتطوير لتكوين أجهزة إستشعار شبكة Cisco Systems وأجهزة إستشعار IPS للمحول ووحدات شبكة IPS للموجهات وبرامج منع الاقتحام المضمنة في الموجهات. يسمح مركز إدارة CiscoWorks لأجهزة إستشعار IPS للمسؤولين بتوفير الوقت من خلال تكوين أجهزة إستشعار متعددة في نفس الوقت باستخدام ملفات تعريف المجموعة. بالإضافة إلى ذلك، فإنه يوفر ميزة إدارة توقيع فعالة تزيد من الدقة والتحديد في اكتشاف الاختراقات المحتملة للشبكة.

ارجع إلى إصدارات البرامج والأجهزة المدعومة لمركز الإدارة لوثائق أجهزة إستشعار IPS للحصول على معلومات التوافق.

مركز مراقبة الأمان (SecMon) من CiscoWorks

يعد مركز مراقبة CiscoWorks للأمان أداة لالتقاط أحداث الأمان من:

- نظام منع التسلل (IPS) لشبكة Cisco

- معرفات شبكة Cisco
- معرفات المحولات من Cisco
- موجهات Cisco IOS مع وظائف IPS المضمنة
- الوحدات النمطية للموجات IDS من Cisco
- جدران الحماية من الجيل التالي Cisco PIX
- الوحدات النمطية لخدمات جدار الحماية Cisco Catalyst 6500 Series Firewall Services Modules (FWSM))
- مركز إدارة CiscoWorks لعملاء أمان Cisco
- مركز مراقبة CiscoWorks لخوادم الأمان

راجع إصدارات البرامج والأجهزة المدعومة لمركز المراقبة للحصول على وثائق الأمان للحصول على معلومات التوافق.

نظام Cisco لمراقبة الأمان والتحليل والاستجابة (MARS)

نظام تحليل مراقبة الأمان والاستجابة (MARS) من Cisco عبارة عن مجموعة من الأجهزة فائقة الأداء والقابلة للتطوير لإدارة التهديدات ومراقبتها والتخفيف من آثارها، مما يساعد العملاء على تحقيق إستخدام أكثر فعالية للشبكة وأجهزة الأمان. تجمع Cisco Security MARS بين مراقبة حدث الأمان التقليدي وذكاء الشبكة وارتباط السياق وتحليل المتجهات واكتشاف الأخطاء وتعريف النقاط الساخنة وإمكانات التخفيف المؤتمتة. وبالجمع بين هذه القدرات، تساعد ميزة Cisco Security MARS الشركات على تحديد هجمات الشبكة بدقة والقضاء عليها مع الحفاظ على توافق الشبكة في نفس الوقت.

إصدارات مارس	برنامج الجهاز/المستشعر المدعوم
x.3.3	x.3 و x.4
x.3.4	x، 4.x، 5.x.3

راجع ملاحظات إصدار المنتج للحصول على مزيد من المعلومات.

الاستجابة للتهديدات من Cisco (CTR)

تعمل ميزة "الاستجابة للتهديدات من Cisco" (CTR) مع أجهزة إستشعار Cisco IPS لتوفير حل فعال للحماية من التطفل. تؤدي الاستجابة للتهديدات من Cisco إلى القضاء بشكل فعلي على الإنذارات الكاذبة وتصعيد الهجمات الحقيقية وتساعد على إصلاح الاختراقات المكلفة.

تتوافق إستجابة تهديد Cisco مع الإصدار x.3 من Cisco IPS أو إصدار أحدث. راجع ملاحظات إصدار المنتج للحصول على مزيد من المعلومات. أيضا، كن على دراية بإعلان نهاية العمر الافتراضي لاستجابة تهديدات Cisco.

عارض حدث IDS (IEV)

إن عارض أحداث نظام كشف التسلل (IDS) هو تطبيق قائم على تطبيق جافا يمكنك من عرض وإدارة التنبيهات لما يصل إلى خمسة أجهزة إستشعار. باستخدام عارض أحداث IDS يمكنك الاتصال بالتحذيرات وعرضها في الوقت الحقيقي أو في ملفات السجل المستوردة. يمكنك تكوين عوامل التصفية وطرق العرض لمساعدتك في إدارة التنبيهات واستيراد بيانات الأحداث وتصديرها لمزيد من التحليل. يوفر عارض أحداث IDS أيضا الوصول إلى قاعدة بيانات أمان الشبكة (NSDB) لأوصاف التوقيعات.

يتم دعم IEV من IDS الإصدار 3. 1 إلى الإصدار x.4. وعلى الرغم من أنها لم تعد مدعومة من الإصدار x.5، إلا أنه يمكن إستخدامها لمراقبة أجهزة الاستشعار الإصدار x.5. ومع ذلك، لا يتم الإبلاغ عن الخصائص الجديدة 5. 0 بواسطة نظام معلومات التوجيه. راجع أمثلة تكوين المنتج والملاحظات التقنية للحصول على مزيد من المعلومات.

مدير جهاز IDS (IDM)

مدير أجهزة IDS (IDM) هو تطبيق يستند إلى الويب يسمح لك بتكوين جهاز الاستشعار وإدارته. يوجد خادم ويب الخاص بإدارة أجهزة IDS على المستشعر. يمكنك الوصول إليها من خلال مستعرضات الويب Netscape أو Internet Explorer.

يتم دعم IDM من IDS الإصدار 3.1. راجع أمثلة تكوين المنتج والملاحظات التقنية للحصول على مزيد من المعلومات.

مدير السياسة الآمنة (CSPM) من Cisco

يوفر Cisco Secure Policy Manager (CSPM) إدارة أمان قائمة على السياسات لأجهزة إستشعار Cisco IDS وجدران الحماية ل PIX وموجهات IPsec VPN.

ملاحظة: بلغت CSPM قائمة التحكم الخاصة بها. ارجع إلى إعلان EOs/EOI ل Cisco Secure Policy Manager 2.x و x.3.

الطراز	CSPM، الإصدار 2.2	CSPM 2.3i	CSPM 2.3.1i	CSPM 2.3.2i	CSPM 2.3.3i
IDS 4210 IDS 4220 IDS 4230	x.2.2.0 x.2.2.1 (0)2.5	x.2.2.0 x.2.2.1 (0).2.5 S0 S(1)2.5 0 S(1)2.5 2	2.2. x.0 2.2. x.1 .2.5 S(0) 0)2.5 S0(1)2.5 S2(1)3.0 S3(1)3.0 S4(1	2.2 ..0 x 2.2 ..1 x 2.5 0). S0(2.5 (1) S0 2.5 (1) S2 3.0 (1) S3 3.0 (1) S4	x.2.2.0 2.2.1.5 2.5(1)S 3 2.2.1.0 2.2.1.6 S(1)3.0 4 2.2.1.1 S(0)2.5 0 3.0(1)S 5 2.2.1.2 S(1)2.5 0 3.0(1)S 6 2.2.1.3 S(1)2.5 1 3.0(1)S 7 2.2.1.4 S(1)2.5 2 3.0(1)S 8
Catalyst 6000 Intrustion Detection System (Module (IDSM-1	2.5 IDSM	2.5 IDSM	2.5 IDSM 3.0 IDSM	2.5 IDS M 3.0 IDS M	S(0)2.5 0 IDSM 2.5(1)S 2 IDSM S(1)2.5 0 IDSM 3.0(1)S

4 IDSM S(1)2.5 1 IDSM 3.0(1)S 6 IDSM					

مدير UNIX

يوفر مدير UNIX واجهة رسومية مركزية لإدارة الأمان عبر شبكة موزعة. كما يمكنها القيام بوظائف مهمة أخرى مثل إدارة البيانات من خلال أدوات تابعة لجهات خارجية والوصول إلى قاعدة بيانات الشبكة (NSDB) ومراقبة وإدارة أجهزة الاستشعار ووحدات كشف التسلل (IDSM) عن بعد وإرسال صفحات أو رسائل بريد إلكتروني إلى موظفي الأمن عند وقوع أحداث أمنية. تعمل واجهة المدير فوق برنامج OpenView من HP.

ملاحظة: وصل الإصدار x.2.2 من البرنامج لمستشعر جهاز Cisco IDS إلى قائمة التحكم الخاصة به. راجع نهاية العمر الافتراضي لوثائق برنامج مستشعر Cisco IDS 2.2.x.

إصدارات المدير	برنامج الجهاز/المستشعر المدعوم
2.1.1	2.1.1
2.2.0	2.2.0
2.2.1	2.2.1
2.2.2	2-2-2 و 2-5
2-2-3*	2-2-3 و 3-0 و 3-1

* 2.2.3 هو آخر إصدار متوفر من برنامج مدير IDS ويدعم برنامج المستشعر 3.1 والإصدارات الأقدم.

في حين أن مدير x.2.2 قد يكون متوافقا مع إصدارات مستشعر x.2.2 بشكل عكسي، إذا لم يكن لديك على الأقل نفس إصدار البرنامج على كل من المدراء وأجهزة الاستشعار، فقد لا تتوفر وظائف مستشعر أحدث في المدير. وهذا يفرض تكوين سطر أوامر يدويا. ارجع إلى وثائق المنتج للحصول على مزيد من التفاصيل.

معلومات ذات صلة

- نظام Cisco لمنع الاقتحام
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك اكتشاف إقتحام CiscoSecure)

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).