使用Rapid7配置ISE 2.2以威脅為中心的NAC(TC-NAC)

目錄

簡介 必要條件 需求 採用元件 設定 高級流程圖 部署和配置下一掃描程式 步驟1.部署Nexpose Scanner。 步驟2.配置Nexpose Scanner。 配置ISE 步驟1.啟用TC-NAC服務。 步驟2.匯入附屬掃描器證書。 步驟3.配置Nexpresence Scanner TC-NAC例項。 步驟4.配置授權配置檔案以觸發VA掃描。 步驟5.配置授權策略。 驗證 身分識別服務引擎 附件掃描器 疑難排解 ISE上的調試 相關資訊

簡介

本文檔介紹如何使用Identity Service Engine(ISE)2.2上的Rapid7配置以威脅為中心的NAC並對其進 行故障排除。威脅中心網路訪問控制(TC-NAC)功能使您能夠根據從威脅和漏洞介面卡接收的威脅和 漏洞屬性建立授權策略。

必要條件

需求

思科建議您瞭解以下主題的基本知識:

- 思科身分識別服務引擎
- Nexpose漏洞掃描器

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 思科身分識別服務引擎版本2.2
- Cisco Catalyst 2960S交換器15.2(2a)E1
- Rapid7 Nexpose漏洞掃描器企業版
- Windows 7 Service Pack 1
- Windows Server 2012 R2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

高級流程圖



以下是流程:

- 1. 客戶端連線到網路,提供有限的訪問並分配啟用了Assess Vulnerabilities覈取方塊的配置檔案 。
- PSN節點向MNT節點傳送系統日誌消息,確認發生了身份驗證,並且VA掃描是授權策略的結果。
- 3. MNT節點使用以下資料向TC-NAC節點(使用管理WebApp)提交SCAN: -MAC 地址

-IP 位址 — 掃描間隔

- 定期掃描已啟用
- 始發PSN
- 4. Nexpose TC-NAC(封裝在Docker容器中)與Nexpose Scanner通訊以觸發掃描(如果需要)。
- 5. Nexpose Scanner掃描ISE請求的端點。
- 6. Nexpose Scanner將掃描結果傳送到ISE。
- 7. 掃描結果將傳送回TC-NAC:
 - -MAC 地址
 - 所有CVSS分數
 - 所有漏洞(標題、CVEID)
- 8. TC-NAC使用步驟7中的所有資料更新PAN。

9. 如果需要,將根據配置的授權策略觸發CoA。

部署和配置下一掃描程式

注意:本文檔中的附件配置用於實驗目的,請諮詢Rapid7工程師以瞭解設計注意事項

步驟1.部署Nexpose Scanner。

Nexpose掃描器可以從OVA檔案部署,安裝在Linux和Windows作業系統之上。在本文檔中,安裝在Windows Server 2012 R2上完成。從Rapid7網站下載映像並開始安裝。配置**Type and destination**時,請選擇**Nexpose Security Console with local Scan Engine**

	Installer - Nexpose 📃 🗖 🗙	
nexpose	Select components and an installation path	
Welcome License agreement • Type and destination System check User details Database port Account details Shortcut location Confirm selections Installation progress Initialization Console details Installation success	Select only the set of components you want to install. If you want to modify the installation directory, click *Change*. Once you have selected your installation directory click *Next*. Nexpose Security Console with local Scan Engine If you do not have a console installed yet, this option is recommended. The console manages scan engines and all Nexpose operations. Nexpose Scan Engine only This distributed engine can start scanning after being paired with a Nexpose Security Console. Communication Direction: Engine to Console v C:\Program Files\rapid7\nexpose Free disk space: 26,603 MB 	
RAPID	Cancel Previous Next	

安裝完成後,伺服器將重新啟動。啟動後,Nexpose掃描器應可通過3780埠訪問,如下圖所示:

3	Installer - Nexpose
nexpose	Installation is complete!
	Installation is complete!
Welcome License agreement Type and destination System check User details Database port Account details Shortcut location Confirm selections Installation progress Initialization Console details • Installation success	 If you chose to start Nexpose as part of the installation, then it is already running. You can log onto Nexpose at https://localhost:3780, Use the credentials you created during installation. To start scanning, click the Home tab in the Nexpose Security Console Web interface. For quick-start help, click the Help link. NOTE: If you did not select the option to start Nexpose as part of the installation, Nexpose will initialize during first-time startup. This will take 10 to 30 minutes depending on your system capabilities. You can start Nexpose manually by executing C:\Program Files\rapid7\nexpose\nsc\nsc.bat. Nexpose is configured to start automatically. See the installation guide if you wish to modify start modes.
RAPID	Finish

x

如圖所示, scanner將經歷安全控制檯啟動過程:

-53

THE SECURITY CONSOLE IS INITIALIZING, PLEASE WAIT ...

Security Console Startup Progress

11/23/2016, 10:04:26 AM : 32% : Loading content definitions...

之後,要訪問GUI,應提供許可證金鑰。請注意,需要Enterprise Edition of Nexpose Scanner,如 果安裝了Community Edition,則不會觸發掃描。

步驟2.配置Nexpose Scanner。

第一步是在Nexpose掃描器上安裝證書。本文檔中的證書由與ISE(實驗室CA)管理證書相同的

CA頒發。 導航到Administration > Global and Console Settings。在Console下選擇**管理**,如下圖所 示。

≡	nexpose' Create	~				۵	弦	@~	đ	۹	은 admin	5
	은 Users		C Asset Groups	22 Exceptions and Overrides		(ii) o	alendar					
	Create and manage	user accounts or manage custom user roles	Create dynamic or static asset groups and manage existing asset	Review requests to exclude vulner	rabilities from reports and to	View ci	alendar of all s	cheduled sca	ns, blackouts	, database op	perations	
	and password policy		groups.	override policy compliance results	L.	and rep	orts.					
	_											
	Scan Options											
	ENGINES SHARED CREDENTI	Create and manage available Scan ALS Create and manage shared credent	Engines, and Scan Engine Pools. ials for authenticated scans.	HISTORY TEMPLATES	View current and past scans for this Create and manage scan templates	s installation. s for controllin	g and tuning s	cans.				
	BLACKOUTS	Create and manage global blackour	settings.	ROOT CERTIFICATES	Manage root certificates used in sc	anning and w	arehouse expo	irt.				
	_											
	Q. Discovery Opti	ons		Global and Console Settings	:							
	NSX MANAGER	Create and manage settings that giv the NSX OVF distribution.	e a Scan Engine direct access to an NSX network of virtual assets.Update	GLOBAL CONSOLE	Manage global settings for selectin	g risk score si Console, jeci	trategies and e	excluding asse	ets from scar	15.		
	CONNECTIONS	Create and manage connections that	t allow the Security Console to discover assets dynamically.	GONDOLL	Parimeter act ingation one decarry	Console, mor	and a set of the	aave ana iogg	ng secongs.			
	EVENTS	View events and statistics for asset	discovery mechanisms.									

按一下「Manage Certificate」,如下圖所示:

≡	nexpose®	Create 🗸				
Û						
	Securi	ty Console Conf	figuration			
Ţ	GENERAL		The Security Console contains an embedded	l web server. The fo	ollowing web server settings can be configured.	
受	UPDATES		WEB SERVER SETTINGS			
\oslash	WEB SERVER		Web server port	β780		
æ	PROXY SE	TTINGS	Session timeout (seconds)	600		
Ø	AUTHENT	ICATION	Initial request handler threads	10		
0	DATABASI	E	Failed login threshold	4		
	SCAN ENG	lines	HTTPS certificate	Issued to n	nexpose.example.com	
	LICENSIN	3		Valid until T	Thu Nov 22 01:16:44 PST 2018	
	EXPOSURI	E ANALYTICS		MANAGE CEF	RTIFICATE	

如圖所示,在**建立新證書**中按一下。輸入**Common Name**以及您希望在Nexpose Scanner的身份證 書中包含的任何其他資料。確保ISE能夠使用DNS解析附屬掃描器FQDN。

Manage Certificate

This dialog will create a new self signed SSL certificate to be used by the Security Console web server. The current certificate will be overwritten. The new certificate can then be used 'as-is' or can be signed by a certification authority by generating a Certificate Signing Request (CSR).

Common name (rully qualified domain name)	nexpose.example.com	
Country (two letter country ISO code. e.g. US)		
State/Province		
Locality/City		
Organization		
Organizational unit		
Valid for (years)	10	
_		
	CREATE BACK	

將憑證簽署請求(CSR)匯出到終端。



此時,您需要與憑證授權單位(CA)簽署CSR。

The Security Console has generated a certificate signing request for the current certific the CSR below and send it to your CA for signature. The signed certificate can later be i Security Console using the 'Import Signed Certificate' button.	ate. You may copy mported into the
BEGIN NEW CERTIFICATE REQUEST MIIEYzCCAksCAQAwHjEcMBoGA1UEAxMTbmV4cG9zZS5leGFtcGxlLmNvbTCCAilw DQYJKoZlhvcNAQEBBQADggIPADCCAgoCggIBAIWOyIrdS0IrDwLMaHEISqHZoG4G oyg3oC9MeML7s1TugD0K4pvmlZ0h1E+B6bK7Z0B3QAnf9/VxKaur/Q/yCNj1AcYH GB+Sq4bAfqHFIKlsjdnj3e00LW7h8TPmD57N0z0v4X8v6D0z42YF8TNSmScbeTZ5 q4qc9DH6RuYU0EYawclWs+7wTVRDt+hyFL6v6e6reIXF7NIp8ssqC02ZvDGzLnzb mwJFNG13BILZykhjMzZVsnnGWAn9IghqQRNftXW5JHYdFVs84WeB+DKX1KWneigL rsay1voSprJXjncC3xAXHWQGFknY8d8eoaEM82fUdzz6Y/j0qUH6ToZ5mEAsKINg JEQpzLxjQsnAZRG8dy9+J52S6Zm7RXyCg0p7MRKlykE0MGEqR5TF0ZWCfTxomvzp S0WExoXpWL8oZb0tPHheWaQSmPStzeuQpiFXNjth/XQ0gHpc48v+1DdDeZI/wrLd j84GMbFuYvBq+x08prU/kGEVftVABGHnjnstGN+qM8CU93mq/6NNPmz8XCgAxC0m w/oD2cQFCdp1XBC7cUdvkXMIJwqQXtpd8uz9ZLvK+afJT8cBphledh1Fy+v7Mu+m OeNlx41XDaudLii/SuYBB03DLbN6Inu7Vp+5/3W59lcfmHlt+3oEJAnWx2vVCLgD	

按一下Import Certificate,匯入CA頒發的證書。

This dialog enables you to create and manage the HTTPS certificate used by the Security Console web server. By default the Security Console uses a self-signed X.509 certificate which is created during installation. This certificate can be replaced by a custom self-signed certificate or a certificate signed by a trusted Certification Authority (CA) like Verisign, Thawte or your own CA. You may perform one or more of the following operations:

- Create New Certificate: Create a new self signed SSL certificate to be used by the Security Console web server. The current certificate will be overwritten. The new certificate can then be used 'as-is' or can be signed by a certification authority by generating a CSR.
- Generate CSR: Once you have created a custom certificate you may generate a Certificate Signing Request (CSR) for the current certificate. You may copy the generated CSR and send it to your Certification Authority.
- 3. Import Certificate / Certificate Chain: After you obtain a signed certificate from your CA you may import it to the Security Console. The Security Console will only accept a certificate that matches the current certificate/keypair. Make sure that the certificate has not been changed since you generated the CSR for this certificate.

The signed certificate **must** be based on a Certificate Signing Request generated by the Security Console. The Security Console does not allow you to import an arbitrary keypair/certificate generated by you.

View current certificate.

CLOSE

配置站點。站點包含您應該能夠掃描的資產,並且用於將ISE與附屬掃描器整合的帳戶應具有管理 站點和建立報告的許可權。導覽至Create > Site,如下圖所示。

≡	nexpose	Create 🔨
仑		Asset Group
		Dynamic Asset Group
		Report
_	0	Site
Ŷ	0	Tags

如圖所示,在「Info & Security」索引標籤上輸入Name。Assets頁籤應包含有效資產的IP地址,即 符合漏洞掃描條件的端點。

=	nexpose	Create 🗸						₿ 9×	ර ී admin
	Site Co	nfiguration							SAVE & SCAN SAVE CANCEL
			_	-					
		INFO & SECURITY	ASSETS		TEMPLATES	ENGINES		ALERTS	SCHEDULE
	GENERAL		General						
	ORGANIZAT	TION		No. 64	a tan	~			
	ACCESS			Importance No	ormal	~			
				Description					
									li
			User-added Tags CUSTOM TAGS		LOCATIONS	OWNERS		CRITICALITY	
			None		None	None		None	Add tags
	nexpose	Create 🗸							ල් ී ද දී admin
	Site Co	nfiguration							SAVE & SCAN SAVE CANCEL
						•			-
		INFO & SECURITY	ASSETS		TEMPLATES	¢ ENGINES		ALERTS	SCHEDULE
			×						
	Specify a	Issets by Names/Addres	ses Connection 🕢				_		
	INCLU	DE Accete Resures Ma	file colored			1 assets 😽	EXCL	JDE	0 assets 😽
		Assets Browse No	nie selected.				0	Assets Browse No file selected.	
		10.229.20.32 × Enter name	e, address, or range.					Enter name, address, or range.	
						4	r		

將簽署ISE證書的CA證書匯入到受信任的儲存中。導航到管理>根證書>管理>匯入證書。

≡	nexpose	Create V	8	₩	@~	ф ² ч	≗ admin
							_
	C	ISTOM CERTIFICATES 💿					^ X
		MPORT CERTURICATES					
	D	stinguished Name	SHA-1 Fingerprint			Expires On	Delete
\odot	c	N-LAS CA, DC-example, DC-com	FD729A38B533726FF8450	358A2F7EB27E	C8A1178	02/12/2025	Ē
	PI	RESET CERTIFICATES					
	D	stinguished Name	SHA-1 Fingerprint			Expires On	
	c	N-DigiDert Assured ID Root CA, OU-www.digicert.com, 0-DigiDert Inc, C+US	056388630D62D75A88C8	AB1E48DF85A8	99824043	11/10/2031	
=	c	N+TC TrustCenter Class 2 CA II, 0U+TC TrustCenter Class 2 CA, 0+TC TrustCenter GmbH, C+DE	AE5083ED7CF45CBC8F61	C621FE685D794	221156E	12/31/2025	
	E	AAILADDRESS-premium-server@thawte.com, CN=Thawte Premium Server CA, OU=Certification Services Division, O=Thawte Consulting cc, L=Cape Town, ST=Western Cape, C=ZA	E0AB05942072549305606	2023670F7CD2	FC6666	01/02/2021	

配置ISE

步驟1.啟用TC-NAC服務。

在ISE節點上啟用TC-NAC服務。請注意以下事項:

- 以威脅為中心的NAC服務需要Apex許可證。
- 對於以威脅為中心的NAC服務,您需要單獨的策略服務節點(PSN)。
- •只能在部署中的一個節點上啟用以威脅為中心的NAC服務。
- 對於漏洞評估服務,每個供應商只能新增一個介面卡例項。

dent	ity Services E	ingine _l	Home Co	ontext Visibility	 Operations 	Policy	 Administration 	Work Centers
▼ System	Identity Mar	nagement 🕨	Network Resou	rces I Device F	Portal Managem	ent pxGrid Se	ervices + Feed Se	ervice Threat Centric NAC
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade E	Backup & Restor	e Admin Access	s > Settings
Deploym	ent		<u>نۇن</u> ى	Deployment Nodes Edit Node General Setting	List > ISE22-10	ek g Configuration		
• 💑 D(ployment				Hostname IS FQDN IS IP Address 10 Node Type Ide	E22-1ek E22-1ek.exam .48.23.86 entity Services	ple.com Engine (ISE)	
				Personas				
				Administration	ı		Role STAND	DALONE Make Primary
				Monitoring			Role	MARY
				Policy Service	le Session Servi	Personas	Include Node	e in Node Group None (
				🗹 Enab	le Profiling Serv	ice		
				🗹 Enab	le Threat Centri	c NAC Service	(i)	
				Enab	le SXP Service		Use Interface	GigabitEthernet 0 v
				Enab	le Device Admir	Service	۲	
				Enab	le Passive Ident	ity Service	۲	
				pxGrid (i)				

步驟2.匯入附屬掃描器證書。

將Nexpose Scanner CA證書匯入思科ISE中的受信任證書庫(Administration > Certificates > Certificate Management > Trusted Certificates > Import)。確保在思科ISE受信任證書儲存中匯入 (或存在)相應的根證書和中間證書

dentity Services Engine	Home Context Visibility Operations Polic	y ▼Administra	ation Work Centers						Licens
▼System Identity Management	Network Resources	id Services F	eed Service + Threat Cen	tric NAC					Click here to do wireless setu
Deployment Licensing Certificates Logging Maintenance Upprade Backup & Restore Admin Access Settings									
0									
- Certificate Management	Trusted Certificates								
System Certificates	/ Edit Import Export XDelete View								S
Trusted Certificates	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
OCSP Client Profile	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro	Baltimore CyberTrust Ro	Fri, 12 May 2000	Tue, 13 May 2025	2
Certificate Signing Requests	Cisco CA Manufacturing	Ø Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00	Cisco Manufacturing CA	Cisco Root CA 2048	Sat, 11 Jun 2005	Mon, 14 May 2029	
Certificate Periodic Check Setti	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	~
Certificate Authority	Cisco Root CA 2048	Ø Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029	
	Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	2
	Default self-signed server certificate	Enabled	Endpoints Infrastructure	58 08 8E 16 00 00	ISE22-1ek.example.com	ISE22-1ek.example.com	Thu, 20 Oct 2016	Fri, 20 Oct 2017	
	DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A3	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 2021	
	LAB CA#LAB CA#00005	Enabled	Infrastructure Endpoints	2F DB 38 46 B8 6D	LAB CA	LAB CA	Thu, 12 Feb 2015	Wed, 12 Feb 2025	
	NeXpose Security Console#NeXpose Security Consol	Enabled	Infrastructure Cisco Services Endpoints	-C 49 10 5A 46 EB	NeXpose Security Console	NeXpose Security Console	Fri, 18 Nov 2016	Wed, 18 Nov 2026	
	Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5	thawte Primary Root CA	thawte Primary Root CA	Fri, 17 Nov 2006	Thu, 17 Jul 2036	
	VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D	VeriSign Class 3 Public	VeriSign Class 3 Public	Wed, 8 Nov 2006	Thu, 17 Jul 2036	
	VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03	VeriSign Class 3 Secure	VeriSign Class 3 Public	Mon, 8 Feb 2010	Sat, 8 Feb 2020	

步驟3.配置Nexpresence Scanner TC-NAC例項。

在Administration > Threat Centric NAC > Third Party Vendors 處新增Rapid7例項。

cisco Iden	tity Services Engir	10 Home	Context Visibility	 Operations 	Policy	▼Adminis	stration	Work Centers
System	Identity Manager	nent • Network	Resources • Dev	ice Portal Management	t pxGrid S	ervices	Feed Service	e ▼Threat Centric NAC
Third Party	Vendors							
Vendor Ins Input fields	stances > New s marked with an aste	risk (*) are required	j.					
	Vendor	Hapid7 Nexpose :	VA			•		
	Instance Name *	Rapid7						
				C	ancel	ave		

新增例項後,例項將轉**至Ready to Configure**狀態。按一下此連結。配置**Nexpose Host**(Scanner)和 Port,預設情況下為3780。指定**Username**和Password,以便訪問正確的站點。

Enter Nexpose Security Console credentials

nexpose.example.com	
The hostname of the Nexpose Security Console Host.	
Nexpose port	
3780	
The port of the Nexpose Security Console host.	
Username	
admin	
Username to access Nexpose Security Console.	
Password	
•••••	
Password of the user.	
Http proxy Host	
Optional http proxy host. Requires proxy port also to I	be set.

Optional http proxy port. Requires proxy host also to be set.



高級設定在ISE 2.2管理指南中有詳細記錄,可以在本文檔的參考部分找到連結。按一下Next和 Finish。Nexpose例項轉換為Active狀態並開始下載知識庫。

cisco Ide	entity Services Engine	Home Context	t Visibility ► Op	perations Policy	- Administration	Work Centers	
System	 Identity Managemen 	t Network Resources	Device Portal I	Management pxGrid Servi	ices Feed Service		
Third Part	ty Vendors						
Vendor C Re	fresh 🕂 Add 💼 T	T rash ▼ ⓒ Edit Res	tart Stop			▼ Filter ▼	¢ •
	Instance Name	Vendor Name	Туре	Hostname	Connectivi	ty Status	
	Rapid7	Rapid7 Nexpose	VA	nexpose.example.com	Connected	Active	

步驟4.配置授權配置檔案以觸發VA掃描。

導航到Policy > Policy Elements > Results > Authorization > Authorization Profiles。新增新配置檔 案。在Common Tasks下,選中Vulnerability Assessment覈取方塊。應根據網路設計選擇按需掃描 間隔。

授權配置檔案包含這些av對:

cisco-av-pair = on-demand-scan-interval=48

cisco-av-pair = periodic-scan-enabled=0

cisco-av-pair = va-adapter-instance=c2175761-0e2b-4753-b2d6-9a9526d85c0c

它們被傳送到訪問接受資料包中的網路裝置,儘管它們的真正目的是告訴監控(MNT)節點應該觸發 掃描。MNT指示TC-NAC節點與附件掃描程式通訊。

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Global Exceptions Policy Authenticatio	n Authorization Profiling Posture Client Provisioning Policy Elements
Dictionaries Conditions Results	
0	* Name Rapid7
Authentication	Description
- Authorization	* Access Type ACCESS_ACCEPT T
Authorization Profiles	Network Device Profile 🚓 Cisco 💌 🕀
Downloadable ACLs	Sanijaa Tamplata
▶ Profiling	Track Movement
▶ Posture	Passive Identity Tracking (
Client Provisioning	
	Common Tasks Assess Vulnerabilities Adapter Instance Trigger scan if the time since last scan is greater than 48 Enter value in hours (1-9999) Advanced Attributes Settings iii Select an item I

步驟5.配置授權策略。

- 配置授權策略以使用步驟4中配置的新授權配置檔案。導航到Policy > Authorization > Authorization Policy,找到Basic_Authenticated_Access規則,然後按一下Edit。將許可權從 PermitAccess更改為新建立的Standard Rapid7。這將導致對所有使用者的漏洞掃描。在 Save中按一下。
- 為隔離的電腦建立授權策略。導航到Policy > Authorization > Authorization Policy > Exceptions並建立例外規則。現在,導航到條件>建立新條件(高級選項)>選擇屬性,向下滾動並選擇威脅。展開Threat屬性並選擇Nexpose-CVSS_Base_Score。將運算子更改為大於,然後根據您的安全策略輸入一個值。隔離授權配置檔案應授予對易受攻擊的電腦的有限訪問許可權。

ldentity	Services Engine Home	Context Visibility > Operations Policy > Administration > Work	r Contens	License Warning
al Evenatio	an Deline Authoritection Author	Desting Desting Client Desting > Deline Desting	n van koka	
a Exception	Autority Autoritication Autor	zatori Floring Postare Crent Flovisioning Protoy Elements		Click here to do wireless setup and visibility setup Do no
orizatio	Policy			
the Author	rization Policy by configuring rules base	ed on identity groups and/or other conditions. Drag and drop rules to change the order		
olicy Export	go to Administration > System > Back	up & Restore > Policy Export Page		
Matched R	ule Applies v			
Exception	e (1)			
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
	Exception Rule	Threat-Rapid7 Nexpose-CVSS Base Score GREATER 1	then Quarantine	
_				
andard				
Status	Bule Name	Conditions (identity groups and other conditions)	Permissions	
	Wireless Black List Default	If Blacklist AND Wireless Access	then Blackhole Wireless Access	
-				
<u>~</u>	Profiled Cisco IP Phones	Cisco-IP-Phone	then Cisco_IP_Phones	
~	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones	
0	Compliant_Devices_Access	If (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess	
-	Employee EAD TI P	H (Mireless 802 1V AND BVOD Is Desistered AND EAD TI & AND	then Bermittanese AND BYOD	
0	Elliployee_EXP+1C3	MAC_in_SAN)	alen Permakaes And Brod	
0	Employee_Onboarding	If (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD	
	Wired Guest Access	(Guest Flow AND Wired MAB)	then PermitAccess AND Guests	
-				
~	Wi-Fi_Guest_Access	If (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests	
~	Wired_Redirect_to_Guest_Login	If Wired_MAB	then Cisco_WebAuth	
0	Wi-Fi_Redirect_to_Guest_Login	if Wireless_MAB	then Cisco_WebAuth	
	Basic_Authenticated_Access	If Network_Access_Authentication_Passed	then Rapid7	
-	Default	If an analytical them Descriptions		
×	Delault	in no matches, then DenyAccess		

驗證

身分識別服務引擎

第一個連線觸發VA掃描。掃描完成後,如果匹配了CoA Reauthentication,將觸發CoA Reauthentication應用新策略。

diala Ider	ntity Services Engine	Home + Conte	xt Visibility	* Operations	Policy Adm	ninistration + W	ork Centers							License	Warning 🔺 🔍 🔍	0 0 0
▼ RADIUS	Threat-Centric NAC Live	Logs + TACACS	Troubleshood	t Adaptive	Network Control Rep	ports							Click here to do v	wireless setup a	and visibility setup Do	not show this again. ×
Live Logs	Live Sessions															
		Misconfigured Su	pplicants O		Misconfigured Net	twork Devices O		RADIUS Drops	0	CI	lent Stopped Responding 0		Repeat Cou	nter O		
		0			C)		0			0		0			
											Refresh	Every 1 minute	• Show La	test 20 record	ds 🔹 Within L	ast 24 hours
C Refres	h O Reset Repeat Coun	ts 🚨 Export To 🕶														▼ Filter • • • •
Tim	e	Status	Details	Repeat	Identity	Er	ndpoint ID	Endpoint P	Authenticat	Authorizati	Authorization Profiles	IP Address	Network	Device	Device Port	Identity Group
×		Status			Identity	E	ndpoint ID	Endpoint Prof	Authentication	Authorization	Authorization Profiles	IP Address	• Network	Device	Device Port	Identity Group
Nov	24, 2016 01:45:41.438 PM	0	0	0	alice	30	:97:0E:52:3F:D9	Nortel-Device	Default >> D	Default >> E	Quarantine	10.229.20.32			FastEthernet1/0/5	
Nov	24, 2016 01:45:40.711 PM	~	0		alice	30	:97:0E:52:3F:D9	Nortel-Device	Default >> D	Default >> E	Quarantine	10.229.20.32	Switch_2	960	FastEthernet1/0/5	Profiled
Nov	24, 2016 01:45:39.166 PM	S	0			30	:97:0E:52:3F:D9						Switch_2	960		
Nov	24, 2016 01:32:00.564 PM	~	0		alice	30	:97:0E:52:3F:D9		Default >> D	Default >> B	Rapid7	10.229.20.32	Switch_2	960	FastEthernet1/0/5	

若要驗證檢測到哪些漏洞,請導覽至**Context Visibility > Endpoints**。使用Nexpose Scanner為其提 供的分數檢查每個終端的漏洞。

cisco Id	entity S	ervices En	igine	Home		▶ Opera	tions ▶ Pol	icy ▶ Admir	nistration	Work Centers
Endpoin	ts Us	ers Netw	ork Device	S						
Endpoir	nts > 30):97:0E:52:	3F:D9							
				~	-					
3C:9	97:0E:	52:3F:D	9	20	8					
	ì	MAC Addi Username Endpoint P Current IP Location:	ress: 3C:9 : alice Profile: No ? Address: Location -	7:0E:52:3F rtel-Device 10.229.20.3 ◆ All Loca	:D9 32 tions					
	Applic	ations	Attribute	es /	Authentication	Threats	Vulnerabilitie	s		
ssl-cv	e-2016-2	183-sweet	32					_		
Title:		TLS/SSL E	Birthday att	acks on 64	-bit block ciphers (SWI	EET32)				
CVSS	score:	5								
CVEI	DS:	CVE-2016	-2183							
Repor	ted by:	Rapid7 Ne	xpose							
Repor	ted at:	Thu Nov 24	4 05:42:52	CET 2016						
ssl-st	atic-key-	ciphers								
Title:		TLS/SSL S	Server Sup	ports The L	Jse of Static Key Ciphe	ers				
CVSS	score:	2.5999999								
CVEI	DS:									
Repor	ted by:	Rapid7 Ne	xpose							
Repor	ted at:	Thu Nov 24	4 05:42:52	CET 2016						
rc4-cv	/e-2013-:	2566								
Title:		TLS/SSL S	Server Sup	ports RC4	Cipher Algorithms (CV	E-2013-2566)				
CVSS	score:	4.3000001	9							
CVEI	DS:	CVE-2013	-2566							
Repor	ted by:	Rapid7 Ne	xpose							
Repor	ted at:	Thu Nov 24	4 05:42:52	CET 2016						

在Operations > TC-NAC Live Logs中,您可以檢視應用的授權策略以及CVSS_Base_Score的詳細 資訊。

ahaha cisco	Identity Services Engine Home	Context Visibility Operat	ions Policy	Administration	Work Center	3			License Warning 🔺	۹ و	•	5
RADIUS Threat-Centric NAC Live Logs Toubleshoot Adaptive Network Control Reports							Click here to do wireless setup and visibility setup	Do not show thi	ns again.	×		
Threa	t Centric NAC Livelog											
C F	efresh 🚨 Export To 👻 📕 Pause									▼ Filter ▼	۰.	
	Time	Endpoint ID	Username	Incident type	Vendor	Old Authorization profile	New Authorization profile	Authorization rule matched	Details			
×		Endpoint ID	Username	Incident type	Vendor	Old Authorization profile	New Authorization profile	Authorization rule matched				
	Thu Nov 24 2016 13:45:40 GMT+0100 (C	3C:97:0E:52:3F:D9	alice	vulnerability	Rapid7	Rapid7	Quarantine	Exception Rule	CVSS_Base_Score: 5 CVSS_Temporal_Score: 0			

附件掃描器

當TC-NAC附件掃描觸發VA掃描轉變為**In-Progress**狀態,並且掃描器開始探測端點時,如果您在端 點上運行wireshark捕獲,此時您會看到端點與掃描器之間的資料包交換。掃描程式完成後,結果可 在**首頁**下找到。

SITES										
Name	Assets	Vulnerabilities	Risk 🗸		Scan Engine	Туре	Scan Status	Scan	Edit	Delete
TAC AAA	1	10	1	2,016	Local scan engine	Static	Scan finished on Thu, Nov 24th, 2016	C	0	1
CREATE SITE										

在Assets頁面下,您可以看到有新的終端可用於掃描結果,已標識作業系統,並且檢測到10個漏洞。



當您按一下終端的IP地址時,Nexpose Scanner將帶您進入新的選單,您可以在其中看到包括主機 名、Risc評分和漏洞詳細清單在內的詳細資訊

	nex	pose	Create										@~ (5° a		admin
ô																🖾 ITEMS 🗸
800		TAC	AAA View all s	sites												
Q																
4			ADDRESSES	10.229.20.32	OS	Kicrosoft Windows	RISK SCO	Æ Ø			US	SER-ADDED T	AGS 🔞			
Â			HARDWARE	Unknown	CPE		ORIGIN	AL 6		CUSTOM TAGS			OWN	ERS		
Ø			ALIASES	TAC-PC	LAST SCAN	Nov 24, 2016 4:42:07 AM (6 minutes ago)	2,01	0		None			Nor	1e		
Q			UNIQUE	Unknown	NEXT SCAN	Not set	CONTEXTE	RIVEN		LOCATIONS			CRITIC	ALITY		Add tags
Ø			IDENTIFIERS	710.111			2,01	6		None			Nor	ne		
			SHE	INC MA												
Ø			SCAN ASSET NOV	W CREATE ASSET REPORT DELETE ASSET	SEND LOG											
⊨																_
≡	nexp	ose	Create											đ		😤 admin
Û																
88		VU Vie Exp	ULNERABILITIE w details about die sosures: 發 Susc	S scovered vulnerabilities. To use one of the exception controls eptible to malware attacks 🖗 Metasploit-exploitable 🖏 Va	on a vulnerability, se slidated with Metasp	lect a row. To use the control with all displayed displayed vulners $\tilde{\mathbf{b}}$ Validated with published exploit	bilities, select the top row and	use Select	Visible. Canc	el all selections using Clear All. 👩)					
88 🖵		VU Vie Exp	ULNERABILITIE w details about dit posures: & Susc EXCLUDE	IS scovered vulnerabilities. To use one of the exception controls eptible to malware attacks @ Metasploit exploitable @ Va RECALL RESUBNIT	on a vulnerability, se vlidated with Metasp	lect a row. To use the control with all displayed displayed winers on 🔮 Exploit published 👋 Validated with published exploit	bilities, select the top row and	use Select	Visible. Canc	el all selections using Clear All. 👩	,		To	tal Vulnerabil	ities Sele	ted:0 of 10
品		VU Vie Exp	ULNERABILITIE www.details.about.dis possures: & Susc EXCLUDE CTITLE	IS scovered vulnerabilities. To use one of the exception controls eptible to malware attacks @ Metaspion-explosible @ Via RECALL RESUBMIT	on a vulnerability, se alidated with Metasp	lect a row. To use the control with all displayed displayed vulners on $\underline{\mathcal{A}}$. Exploit published $\widehat{\mathcal{A}}$ Validated with published exploit	abilities, select the top row and	use Select	Visible. Canc CVSS	el all selections using Clear All. 🗑 Risk Published On	Me	odified On	To Severity ~	tsl Winersbil Instances	ities Sele	sted: 0 of 10
명 · · · · · · · · · · · · · · · · · · ·		Vie Exp	ULNERABILITIE w details about dis possures: Susc EXCLUDE - Title TLS/SSL Bir	IS scovered vulnerabilities. To use one of the exception controls eptible to malware attacks @ Metaspiont-explorable @ Via RECALL RESUBMIT thday attacks on 64-bit block ciphers (SWEET32)	on a vulnerability, se ilidated with Metasp	tect a row. To use the control with all displayed displayed volners of The Exploit published and Walidated with published exploit	ubilities, select the top row and	use Select	Visible. Canc CVSS 5	el all selections using Clear All. @ Risk Published On 425 Wed Aug 24	0 Mc 2016 Fri	odified On Sep 02 2016	To Severity ~ Severe	tel Winerabil Instances	Itles Selec Exce 1 Ø	sted: 0 of 10 ptions Exclude
B ↓ ★ ⊘		VU Exp	ULNERABILITIE www.details.about.dis coosures: & Susc EXCLUDE - Table - Table - TLS/SSL Bir - TLS Server 5	IS Sovernd vulnerabilities. To use one of the exception controls eptible to malwere attacks @ Metasploit explorable @ Via RECALL RESUBMIT thday attacks on 64-bit block ophers (SWEET32) Rupports TLS version 1.0	on a vulnerability, se alidated with Metasp	tect a row. To use the control with all displayed displayed vulners of 3. Exploit published a Validated with published exploit	bilities, select the top row and	use Select 1	Visible. Cano CVSS 5 4.3	Risk Published On 425 Wed Aug 24 324 Tue Det 14 20	0 2016 Fri 2014 Th	odified On Sep 02 2016 u Nov 12 2015	Severity ~ Severe Severe	tal Vulnerabil Instances	ties Selec Exce 1 @ 1 @	ted: 0 of 10 ptions Exclude Exclude
8 8 8 8		Vu Exp	ULNERABILITIE w details about dis cosures: Susc EXCLUDE + Title TLS/SSL Bir TLS/SSL Bir TLS/SSL Server 5	S Sovernd vulnerabilities. To use one of the exception controls eptible to malware attacks W Matasploit-explorable V Va RECALL RESUBMIT thday attacks on 64-bit block ciphers (SWEET32) bitponts TLS version 1.0 rvvr Supports RC4 Cipher Algorithms (CVE-2013-2566)	on a vulnerability, se	lect a row. To use the control with all displayed displayed withers on 3. Exploit published in Validated with published exploit	abilities, select the top row and	use Select 1	Visible. Canc CVSS 5 4.3 4.3	Risk Published On 425 Wed Aug 24 324 Tue 0e1 142 397 Tue Mar 12 2	Mc 2016 Fri 214 Th 013 Th	udified On Sep 02 2016 u Nov 12 2019	To Severity v Severe Severe Severe Severe	tal Vulnerabil Instances	Eles Selec Exce 1 @ 1 @ 1 @	sted: 0 of 10 ptions Exclude Exclude
S () ★ () = =			ULNERABILITIE www.details.about.dis cosures: & Susc EXCLUDE - Title - Titls/SSL Bir - TLS/SSL Se - TLS/SSL Se - TLS/SSL Se	S scovered vulnerabilities. To use one of the exception controls septible to malwere attacks @ Metasploit-exploitable @ Via RECALL RESUBART thday attacks on 64-bit Block ciphers (SWEET32) alugoonts TLS version 1.0 rver Supports RC4 Opher Algorithms (CVE-2013-2566) rver is enabling the BEAST attack	on a vulnerability, se alidated with Metasp	lect a row. To use the control with all displayed displayed wuhers on 3. Exploit published 👋 Validsted with published exploit	abilities, select the top row and	use Select 1	Visible. Canc CVSS 5 4.3 4.3 4.3	Risk Published On 425 Wed Aug 24 324 Tue 0ct 14 2 397 Tue Mar 12 2 448 Tue 5ep 05 2	Mc 2016 Fri 2014 Th 013 Th 011 Th	odified On Sep 02 2016 u Nov 12 2015 u Apr 28 2016 u Feb 18 2016	To Severity v Severe Severe Severe Severe Severe	Instances	Eles Ster Exer 1 @ 1 @ 1 @ 1 @	sted: 0 of 10 ptions Exclude Exclude Exclude
			ULNERABILITIE w details about dis oosures:	S Covered vulnerabilities. To use one of the exception controls expetible to malware attack	on a vulnerability, se alidated with Metasp	lect a row. To use the control with all displayed displayed withers on a Exploit published and Validated with published exploit	abilities, select the top row and	use Select 1	Visible. Canc CVSS 5 43 43 43 2.6	Risk Published On 425 Wed Aug 24 327 Tue 0c1 14 2 397 Tue Mar 12 2 448 Tue Spo 62 910 Wed May 20	Mc 2016 Fri 2014 Th 013 Th 011 Th 2015 Th	odified On Sep 02 2016 u Nov 12 2015 u Apr 28 2016 u Feb 18 2016 u Jun 16 2016	Severe Severe Severe Severe Severe Severe Moderate	Instances	Exce 1 @ 1 @ 1 @ 1 @ 1 @	sted: 0 of 10 ptions Exclude Exclude Exclude Exclude Exclude
® ⊡ & ⊘ & ⊡ ®			ULNERABILITIE w details about di opsaures: Succupe EXCLUPE TILS/SSL Bin TLS/SSL Se TLS/SSL Se TLS/SSL Se Diffie Helim	S Covered vulnerabilities. To use one of the exception controls epithe to malware attack	on a vulnerability, se	iect a row. To use the control with all displayed displayed winners on 走 Exploit published n Validated with published exploit	ablities, select the top row and	use Select	Visible. Canc CVSS 5 4.3 4.3 2.6 2.6	Risk Published On Risk Wed Aug 24 324 Tue Oct 14 20 397 Tue Mer 12 2 448 Tue Sep 65 2 91.0 Wed May 20 91.0 Wed May 20	Mo 2016 Fri 2014 Th 013 Th 011 Th 2015 Th 2015 Th	odified On Sep 02 2016 u Nov 12 2019 u Apr 28 2016 u Feb 18 2016 u Jun 16 2016 u Nov 12 2019	Severity - Severe Severe Severe Severe Severe Moderate Moderate	tal Vulnerabil	ttes Selec Exce 1 0 1 0 1 0 1 0 1 0 1 0 1 0	tind: 0 of 10 ptions Exclude Exclude Exclude Exclude Exclude Exclude Exclude
			LINERABILITIE w details about dis consures: Susc Exclude Title Title TitleState TitleState TitleState TitleState Diffe-Hellin TitleState Diffe-Hellin TitleState	S S scovered vulnerabilities. To use one of the exception controls specifie to malware attack	on a vulnenability, se alidated with Metasp	iect a row. To use the control with all displayed displayed winners on 走 Exploit published n Validated with published exploit	abilities, select the top row and	use Select 1	Visible. Cance CVSS 5 4.3 4.3 2.6 2.6 2.6 2.6	Risk Published On 425 Wed Aug 24 327 Tue Not 14 4 329 Tue Oct 14 2 448 Tue Sep 06 2 91.0 Wed May 20 91.0 Wed May 20 0.0 Extended to the first of the	Mc 2016 Fri 214 Th 013 Th 2013 Th 2015 Th 2015 Th 2015 Th 2015 We	odified On Sep 02 2016 u Nov 12 2019 u Apr 28 2016 u Feb 18 2016 u Jun 16 2016 u Nov 12 2019 d Sep 30 2011	Severity ~ Severe Severe Severe Severe Severe Severe Moderate Moderate Moderate	tal Vulnerabil	Hess Selection 1 2000 1	sted: 0 of 10 rptions Exclude Exclude Exclude Exclude Exclude Exclude
88 ▶ 🛠 ⊘ 🔉 🖸 ⊗ 📖			LNERABILITIE w details about dis consures: Suscent EXCLUDE Title TLS/SSL Bir TLS/SSL Server 1 TLS/SSL Server 1 T	S Covered vulnerabilities. To use one of the exception controls epithe to malware attack	on a vulnerabilty, se	iect a row. To use the control with all displayed displayed winners of " 孟 Exploit published " 我 Validated with published exploit	ablities, select the top row and	use Select 1	Visible, Canco CVSS 5 43 43 43 2.6 2.6 2.6 2.6 0 0	Risk Published On Risk Published On 425 Wed Aug 24 247 Tue Ved 14 22 247 Tue Ved 14 22 2497 Tue Ved 14 22 24910 Wed May 20 240 Sun Feb 0 12 240 Sun Feb 0 12 240 Sun Feb 0 12	Ma 2016 Fri 2014 Th 2013 Th 2015 Th 2015 Th 2015 Th 2015 Th 2015 Th 2015 We 977 Th	odified On Sep 02 2016 u Nov 12 2015 u Apr 28 2016 u Feb 18 2016 u Jun 16 2016 u Nov 12 2015 d Sep 30 201 u Jul 12 2012 u Jul 12 2012	Severe Severe Severe Severe Severe Severe Moderate Moderate Moderate Moderate	tal Vulnerabil Instances	des Selec Dec 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0	stat: 0 of 10 ptons Exclude Exclude Exclude Exclude Exclude Exclude Exclude
88 ▶ ☆ ⊘ ♀ Ⅲ			UNERABILITIE w details about 6 w details about 6 Succure Trate TLS/SSL 8e TLS/SSL 8e TLS/SSL 8e TLS/SSL 8e TLS/SSL 8e TCP timests TCP timests TLS/SSL 9e TLS/SSL 9e	S Covered vulnerabilities. To use one of the exception controls epithe to malware attack	on a vulnerabilty, se	iect a row. To use the control with all displayed displayed winners of " 孟 Exploit published " 我 Validated with published exploit	Ablities, select the top row and	use Select 1	Visible. Canco CVSS 5 4.3 4.3 4.3 2.6 2.6 2.6 0 0 0 0 0	Risk Published On Risk Published On 425 Wed Aug 24 24 Tuo Cut 14 2 397 Tuo Kut 12 397 Tuo Kut 12 397 Tuo Kut 24 397 Tuo Kut 24 391 Wed May 20 391 Wed May 20 391 Wed May 20 391 Wed May 20 391 On Fil Aug 01 391 Fil Aug	Mc 2016 Fri 014 Th 013 Th 2015 Th 2015 Th 2015 Th 015 We 97 Th 014 We 009 Mc	odified On Sep 02 2016 u Nov 12 2019 u Apr 28 2016 u Feb 18 2016 u Jun 16 2016 u Nov 12 2012 rd Sep 30 2011 u Jul 12 2012 rd Dec 10 201- on Feb 15 2011	Severe Severe Severe Severe Severe Severe Moderate Moderate Moderate Moderate	tal Vulnerabil	Lies Science Deve 1 00 1 00 1 00 1 00 1 00 1 00 1 00 1 0	stad. 0 of 10 ptions Exclude Exclude Exclude Exclude Exclude Exclude Exclude Exclude Exclude Exclude
88 🗗 🛠 🛇 🔉 🖸 🖉 🏢			UNERABILITIE w details about di woosares: Succession tracession	S Covered vulnerabilities. To use one of the exception controls prover divulnerabilities. To use one of the exception controls prover by the state of the exception of the exceptio	on a vulnerabilty, se	iect a row. To use the control with all displayed displayed winners on ▲ Exploit published ﴿ Validated with published exploit	abilities, select the top row and	Select '	Visible. Cano CVSS 5 43 43 26 26 26 26 0 0 0 0	Risk Published On 425 Wed Aug 24 425 Wed Aug 24 427 Tue Net 12 42 448 Tue Sep 65 2 449 Tue	McMcR2016 Fri fill Fri fill Th Th Th Th Th Th Th Th Th Th Th Th Th Th Th	odified On Sep 02 2016 u Nov 12 2012 u Apr 28 2016 u Jen 18 2016 u Jen 18 2016 u Jen 12 2012 rd Sep 30 2011 u Jul 12 2012 rd Dec 10 2011 on Feb 15 2010	Severe Severe Severe Severe Severe Moderate Moderate	Instances	Execution Execution 1 Q 1 Q 1 Q 1 Q 1 Q 1 Q 1 Q 1 Q 1 Q 1 Q 1 Q 1 Q 1 Q 1 Q 1 Q 1 Q	tect 0 of 10 ptons Declude Declude Declude Declude Declude Declude Declude Declude Declude Declude

按一下Vulnerability本身時,圖中顯示完整的說明。

	nexpos	e"Create 🗸										، م		admin
														C ITEMS
		VULNERABILITY INFO	RMATION											
		OVERVIEW												
		Title						Severity	Vulnerability ID	CVSS		Published	Modified	
Q		TLS/SSL Birthday attacks of	in 64-bit block ciphers (SWEET3	12)				Severe (5)	ssi-cve-2016-2183-sweet32	5 (AV:N/AC:L/Au:	N/C:P/I:N/A:N)	Aug 24, 2016	Sep 2, 2016	
		DESCRIPTION Legacy block ciphers having should be the exhaustive se with up to 2 to the power of with 64-bit blocks, the birthd	a block size of 64 bits are vuln arch of the key, with complexity n queries, but most modes of o ay bound corresponds to only 3	erable to a practical collision a 2 to the power of k. However, peration (e.g. CBC, CTR, GCM, 2. GB, which is easily reached i	ttack when u the block siz OC8, etc.) ar in practice. C	ised in CBC moo e n is also an im e unsafe with m Ince a collision i	6. All versions of the SQL/TLS protocols that support clother surface operater source) parameter, defining the annuart of data that can be readed to the support and the support of the support of the tenveen two clipher blocks occurs it is possible to use the collision to between two clipher blocks occurs it is possible to use the collision to	which use 3DES as th encrypted under the sund). With a modern o extract the plain te	he symmetric encryption cipher are affect same key. This is particularly important block cipher with 128-bit blocks such as at data.	ed. The security of a when using common AES, the birthday bo	block cipher is ofte modes of operation und corresponds to	n reduced to the k : we require block 256 exabytes. Ho	ry size ic the best atta ciphers to be secure wever, for a block ciph	ick ser
		AFFECTS											_	
		Asset > 10.229.20.32	TAC-PC	TAC AAA	3389	Vulnerable	Negotiated with the following insecure cipher suites:				Las	24th, 2016	Exclude	
						version	TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA							

疑難排解

ISE上的調試

要在ISE上啟用調試,請導航到**管理>系統>記錄>調試日誌配置**,選擇TC-NAC節點,並將**日誌級別** va-runtime和**va-service**元件更改為**DEBUG**。

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
▼System ► Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC
Deployment Licensing + Certificat	es Logging Maintenance Upgrade Backup & Restore Admin Access Settings
G	
Local Log Settings	Node List > ISE21-3ek.example.com Debug Level Configuration
Remote Logging Targets	
Logging Categories	/ Edit Kan Reset to Default
Message Catalog	Component Name Log Level Description
Debug Log Configuration	val 💿
Collection Filters	O va-runtime DEBUG Vulnerability Assessment Runtime messages
	O va-service DEBUG Vulnerability Assessment Service messages

要檢查的日誌 — varuntime.log。您可以直接從ISE CLI對其進行跟蹤:

ISE21-3ek/admin# show logging application varuntime.log tail

TC-NAC Docker收到對特定端點執行掃描的指令。

2016-11-24 13:32:04,436 DEBUG [Thread-94][] va.runtime.admin.mnt.EndpointFileReader -::::- VA: Read va runtime.

[{"operationType":1,"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","ondemandScanInt erval":"48","isPeriodicScanEnabled":false,"periodicScanEnabledString":"0","vendorInstance":"c217 5761-0e2b-4753-b2d6-9a9526d85c0c","psnHostName":"ISE22-1ek","heartBeatTime":0,"lastScanTime":0}, {"operationType":1,"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","isPeriodicScanEnabled":false,"heartBeatTime":0,"lastScanTime":0}]

2016-11-24 13:32:04,437 DEBUG [Thread-94][] va.runtime.admin.vaservice.VaServiceRemotingHandler -:::::- VA: received data from Mnt:

{"operationType":1,"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","ondemandScanInte
rval":"48","isPeriodicScanEnabled":false,"periodicScanEnabledString":"0","vendorInstance":"c2175
761-0e2b-4753-b2d6-9a9526d85c0c","psnHostName":"ISE22-1ek","heartBeatTime":0,"lastScanTime":0}
2016-11-24 13:32:04,439 DEBUG [Thread-94][] va.runtime.admin.vaservice.VaServiceRemotingHandler

漏洞評估請求已提交至介面卡。

ISE21-3ek/admin# show logging application vaservice.log tail

```
2016-11-24 13:45:28,378 DEBUG [Thread-94][] va.runtime.admin.vaservice.VaServiceRemotingHandler
-::::- VA: received data from Mnt:
{ "operationType ":2, "isPeriodicScanEnabled ": false, "heartBeatTime ": 1479991526437, "lastScanTime ": 0 }
2016-11-24 13:45:33,642 DEBUG [pool-115-thread-19][]
va.runtime.admin.vaservice.VaServiceMessageListener -:::::- Got message from VaService:
[{"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","lastScanTime":1479962572758,"vuln
erabilities":["{\"vulnerabilityId\":\"ssl-cve-2016-2183-sweet32\",\"cveIds\":\"CVE-2016-
2183\",\"cvssBaseScore\":\"5\",\"vulnerabilityTitle\":\"TLS/SSL Birthday attacks on 64-bit block
ciphers (SWEET32)\",\"vulnerabilityVendor\":\"Rapid7 Nexpose\"}","{\"vulnerabilityId\":\"ssl-
static-key-
ciphers\",\"cveIds\":\"\",\"cvsBaseScore\":\"2.5999999\",\"vulnerabilityTitle\":\"TLS/SSL
Server Supports The Use of Static Key Ciphers\",\"vulnerabilityVendor\":\"Rapid7
Nexpose\"}","{\"vulnerabilityId\":\"rc4-cve-2013-2566\",\"cveIds\":\"CVE-2013-
2566\",\"cvssBaseScore\":\"4.30000019\",\"vulnerabilityTitle\":\"TLS/SSL Server Supports RC4
Cipher Algorithms (CVE-2013-2566)\",\"vulnerabilityVendor\":\"Rapid7
Nexpose\"}","{\"vulnerabilityId\":\"tls-dh-prime-under-2048-
bits\",\"cveIds\":\"\",\"cvssBaseScore\":\"2.5999999\",\"vulnerabilityTitle\":\"Diffie-Hellman
group smaller than 2048 bits\",\"vulnerabilityVendor\":\"Rapid7
Nexpose\"}","{\"vulnerabilityId\":\"tls-dh-
primes\",\"cveIds\":\"\",\"cvssBaseScore\":\"2.5999999\",\"vulnerabilityTitle\":\"TLS/SSL Server
Is Using Commonly Used Prime Numbers\",\"vulnerabilityVendor\":\"Rapid7
Nexpose\"}","{\"vulnerabilityId\":\"ssl-cve-2011-3389-beast\",\"cveIds\":\"CVE-2011-
3389\",\"cvssBaseScore\":\"4.30000019\",\"vulnerabilityTitle\":\"TLS/SSL Server is enabling the
BEAST attack\",\"vulnerabilityVendor\":\"Rapid7 Nexpose\"}","{\"vulnerabilityId\":\"tlsv1_0-
enabled\",\"cveIds\":\"\",\"cvssBaseScore\":\"4.30000019\",\"vulnerabilityTitle\":\"TLS Server
Supports TLS version 1.0\",\"vulnerabilityVendor\":\"Rapid7 Nexpose\"}"]}]
2016-11-24 13:45:33,643 DEBUG [pool-115-thread-19][]
va.runtime.admin.vaservice.VaServiceMessageListener -:::::- VA: Save to context db,
lastscantime: 1479962572758, mac: 3C:97:0E:52:3F:D9
2016-11-24 13:45:33,675 DEBUG [pool-115-thread-19][]
va.runtime.admin.vaservice.VaPanRemotingHandler -::::- VA: Saved to elastic search:
{3C:97:0E:52:3F:D9=[{"vulnerabilityId":"ssl-cve-2016-2183-sweet32","cveIds":"CVE-2016-
2183", "cvssBaseScore": "5", "vulnerabilityTitle": "TLS/SSL Birthday attacks on 64-bit block ciphers
(SWEET32)","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"ssl-static-key-
ciphers","cveIds":"","cvssBaseScore":"2.5999999","vulnerabilityTitle":"TLS/SSL Server Supports
The Use of Static Key Ciphers", "vulnerabilityVendor": "Rapid7 Nexpose" }, { "vulnerabilityId": "rc4-
cve-2013-2566", "cveIds": "CVE-2013-
2566", "cvssBaseScore": "4.30000019", "vulnerabilityTitle": "TLS/SSL Server Supports RC4 Cipher
Algorithms (CVE-2013-2566)","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"tls-dh-
prime-under-2048-bits", "cveIds":"", "cvssBaseScore":"2.5999999", "vulnerabilityTitle":"Diffie-
Hellman group smaller than 2048 bits", "vulnerabilityVendor": "Rapid7 Nexpose" },
{"vulnerabilityId":"tls-dh-
primes", "cveIds":"", "cvssBaseScore":"2.5999999", "vulnerabilityTitle":"TLS/SSL Server Is Using
Commonly Used Prime Numbers", "vulnerabilityVendor": "Rapid7 Nexpose" }, { "vulnerabilityId": "ssl-
cve-2011-3389-beast", "cveIds": "CVE-2011-
3389", "cvssBaseScore": "4.30000019", "vulnerabilityTitle": "TLS/SSL Server is enabling the BEAST
attack","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"tlsv1_0-
enabled", "cveIds":"", "cvssBaseScore":"4.30000019", "vulnerabilityTitle":"TLS Server Supports TLS
version 1.0","vulnerabilityVendor":"Rapid7 Nexpose"}]}
要檢查的日誌 — vaservice.log。您可以直接從ISE CLI對其進行跟蹤:
```

收到結果後,它會將所有漏洞資料儲存在上下文目錄中。

abled":false,"heartBeatTime":0,"lastScanTime":0}

-::::- VA: received data from Mnt: {"operationType":1,"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","isPeriodicScanEn

cpm.va.service.processor.AdapterMessageListener -::::- Message from adapter : {"returnedMacAddress":"","requestedMacAddress":"3C:97:0E:52:3F:D9","scanStatus":"ASSESSMENT_SUCC ESS","lastScanTimeLong":1479962572758,"ipAddress":"10.229.20.32","vulnerabilities":[{"vulnerabil ityId":"tlsv1_0-enabled","cveIds":"","cvssBaseScore":"4.30000019","vulnerabilityTitle":"TLS Server Supports TLS version 1.0", "vulnerabilityVendor": "Rapid7 Nexpose" }, { "vulnerabilityId": "rc4-cve-2013-2566", "cveIds": "CVE-2013-2566", "cvssBaseScore": "4.30000019", "vulnerabilityTitle": "TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)", "vulnerabilityVendor": "Rapid7 Nexpose" }, { "vulnerabilityId": "ssl-cve-2016-2183-sweet32", "cveIds": "CVE-2016-2183", "cvssBaseScore": "5", "vulnerabilityTitle": "TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)", "vulnerabilityVendor": "Rapid7 Nexpose" }, { "vulnerabilityId": "ssl-static-keyciphers", "cveIds":"", "cvssBaseScore": "2.5999999", "vulnerabilityTitle": "TLS/SSL Server Supports The Use of Static Key Ciphers", "vulnerabilityVendor": "Rapid7 Nexpose" }, { "vulnerabilityId": "tlsdh-primes", "cveIds":"", "cvssBaseScore":"2.5999999", "vulnerabilityTitle":"TLS/SSL Server Is Using Commonly Used Prime Numbers", "vulnerabilityVendor": "Rapid7 Nexpose" }, { "vulnerabilityId": "tls-dhprime-under-2048-bits", "cveIds": "", "cvssBaseScore": "2.59999999", "vulnerabilityTitle": "Diffie-Hellman group smaller than 2048 bits", "vulnerabilityVendor": "Rapid7 Nexpose" }, { "vulnerabilityId": "ssl-cve-2011-3389-beast", "cveIds": "CVE-2011-3389", "cvssBaseScore": "4.30000019", "vulnerabilityTitle": "TLS/SSL Server is enabling the BEAST attack","vulnerabilityVendor":"Rapid7 Nexpose"}]} 2016-11-24 12:45:33,137 INFO [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener -:::::- Endpoint Details sent to IRF is {"3C:97:0E:52:3F:D9":[{"vulnerability":{"CVSS_Base_Score":5.0,"CVSS_Temporal_Score":0.0},"timestamp":1479962572758,"title":"Vulnerability","vendor":"Rapid7 Nexpose"}]} 2016-11-24 12:45:33,221 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil -::::- VA SendSyslog systemMsg : [{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-NAC.ServiceName", "Vulnerability Assessment Service", "TC-NAC.Status", "VA successfully completed", "TC-NAC.Details", "VA completed; number of vulnerabilities found: 7", "TC-NAC.MACAddress", "3C:97:0E:52:3F:D9", "TC-NAC.IpAddress", "10.229.20.32", "TC-

介面卡獲得CVE以及CVSS分數。

NAC.ServiceName", "Vulnerability Assessment Service", "TC-NAC.Status", "Adapter Statistics", "TC-NAC.Details", "Number of endpoints queued for checking scan results: 0, Number of endpoints queued for scan: 0, Number of endpoints for which the scan is in progress: 1", "TC-NAC.AdapterInstanceUuid", "7a2415e7-980d-4c0c-b5ed-fe4e9fadadbd", "TC-NAC.VendorName", "Rapid7 Nexpose", "TC-NAC.AdapterInstanceName", "Rapid7"]}]

which the scan is in progress: 1"} 2016-11-24 12:36:28,880 DEBUG [endpointPollerScheduler-5][] cpm.va.service.util.VaServiceUtil -:::::- VA SendSyslog systemMsg :

{"AdapterInstanceName":"Rapid7","AdapterInstanceUid":"7a2415e7-980d-4c0c-b5edfe4e9fadadbd","VendorName":"Rapid7 Nexpose","OperationMessageText":"Number of endpoints queued for checking scan results: 0, Number of endpoints queued for scan: 0, Number of endpoints for

cpm.va.service.processor.AdapterMessageListener -::::- Message from adapter :

[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-

2016-11-24 12:36:28,143 DEBUG [SimpleAsyncTaskExecutor-2][]

2016-11-24 12:45:33,132 DEBUG [SimpleAsyncTaskExecutor-2][]

AdapterMessageListener每隔5分鐘檢查一次掃描的狀態,直到掃描完成。

Nexpose", "TC-NAC.AdapterInstanceName", "Rapid7"]}]
2016-11-24 12:32:05,810 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil :::::- VA SendSyslog systemMsg res: {"status":"SUCCESS", "statusMessages":["SUCCESS"]}

NAC.MACAddress","3C:97:0E:52:3F:D9","TC-NAC.IpAddress","10.229.20.32","TC-NAC.AdapterInstanceUuid","c2175761-0e2b-4753-b2d6-9a9526d85c0c","TC-NAC.VendorName","Rapid7

NAC.ServiceName", "Vulnerability Assessment Service", "TC-NAC.Status", "VA request submitted to adapter", "TC-NAC.Details", "VA request submitted to adapter for processing", "TC-

[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-

2016-11-24 12:32:05,783 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil - :::::- VA SendSyslog systemMsg :

NAC.AdapterInstanceUuid","c2175761-0e2b-4753-b2d6-9a9526d85c0c","TC-NAC.VendorName","Rapid7 Nexpose","TC-NAC.AdapterInstanceName","Rapid7"]}] 2016-11-24 12:45:33,299 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil -:::::- VA SendSyslog systemMsg res: {"status":"SUCCESS","statusMessages":["SUCCESS"]}

相關資訊

- 技術支援與文件 Cisco Systems
- ISE 2.2版本說明
- ISE 2.2硬體安裝指南
- ISE 2.2升級指南
- ISE 2.2引擎管理員指南