Configurazione di ISE 2.2 Threat-Centric NAC (TC-NAC) con Rapid7

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Configurazione Diagramma di flusso ad alto livello Distribuire e configurare lo scanner Nexpose Passaggio 1. Distribuire lo scanner Nexpose. Passaggio 2. Configurare lo scanner Nexpose. **Configurare ISE** Passaggio 1. Abilitare i servizi TC-NAC. Passaggio 2. Importare il certificato dello scanner Nexpose. Passaggio 3. Configurare l'istanza TC-NAC di Nexpose Scanner. Passaggio 4. Configurare il profilo di autorizzazione per attivare la scansione VA. Passaggio 5. Configurare i criteri di autorizzazione. Verifica **Identity Services Engine** Scanner Nexpose Risoluzione dei problemi Debug su ISE Informazioni correlate

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi relativi ai sistemi NAC basati sulle minacce con Rapid7 su Identity Service Engine (ISE) 2.2. La funzionalità TC-NAC (Threat Centric Network Access Control) consente di creare criteri di autorizzazione basati sugli attributi di minaccia e vulnerabilità ricevuti dagli adattatori minacce e vulnerabilità.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Cisco Identity Service Engine
- Nexpose Vulnerability Scanner

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Service Engine versione 2.2
- Cisco Catalyst 2960S switch 15.2(2a)E1
- Rapid7 Nexpose Vulnerability Scanner Enterprise Edition
- Windows 7 Service Pack 1
- Windows Server 2012 R2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Diagramma di flusso ad alto livello



Questo è il flusso:

- 1. Il client si connette alla rete, viene concesso un accesso limitato e viene assegnato un profilo con la casella di controllo **Valuta vulnerabilità** abilitata.
- 2. Il nodo PSN invia un messaggio Syslog al nodo MNT per confermare l'autenticazione e l'analisi VA è il risultato dei criteri di autorizzazione.

- 3. Il nodo MNT invia SCAN al nodo TC-NAC (utilizzando Admin WebApp) utilizzando questi dati:
 - -Indirizzo MAC
 - -Indirizzo IP
 - Intervallo di scansione
 - Scansione periodica abilitata
 - PSN di origine
- 4. Nexpose TC-NAC (incapsulato nel contenitore Docker) comunica con lo scanner Nexpose per attivare la scansione, se necessario.
- 5. Nexpose Scanner esegue la scansione dell'endpoint richiesto da ISE.
- 6. Nexpose Scanner invia i risultati della scansione ad ISE.
- 7. I risultati della scansione vengono inviati al TC-NAC:
 - -Indirizzo MAC
 - Tutti i punteggi CVSS
 - Tutte le vulnerabilità (titolo, CVEID)
- 8. TC-NAC aggiorna la PAN con tutti i dati del passaggio 7.
- 9. Il CoA viene attivato se necessario in base ai criteri di autorizzazione configurati.

Distribuire e configurare lo scanner Nexpose

Attenzione: La configurazione di Nexpose in questo documento viene eseguita per scopi di laboratorio. Consultare i tecnici Rapid7 per le considerazioni di progettazione

Passaggio 1. Distribuire lo scanner Nexpose.

Nexpose scanner può essere distribuito da file OVA, installato sul sistema operativo Linux e Windows. In questo documento l'installazione viene eseguita in Windows Server 2012 R2. Scaricare l'immagine dal sito Web Rapid7 e avviare l'installazione. Quando si configura il **tipo e la destinazione**, selezionare **Nexpose Security Console con Scan Engine locale**

3	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	 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 Security Se
Console details Installation success	Destination directory: C:\Program Files\rapid7\nexpose Change Free disk space: 26,603 MB
RAPID	Cancel Previous Next

Al termine dell'installazione, il server viene riavviato. Dopo il lancio, lo scanner Nexpose deve essere accessibile tramite la porta 3780, come mostrato nell'immagine:



Come mostrato nell'immagine, lo scanner esegue il processo di avvio della console di sicurezza:



Quindi, per accedere alla GUI, occorre fornire la chiave di licenza. Si noti che è richiesta l'edizione Enterprise di Nexpose Scanner, le analisi non vengono attivate se è installata l'edizione Community.

Passaggio 2. Configurare lo scanner Nexpose.

Il primo passaggio consiste nel reinstallare il certificato su Nexpose Scanner. Il certificato descritto in questo documento viene emesso dalla stessa CA che ha emesso il certificato di amministratore per ISE (LAB CA). Selezionare **Amministrazione > Impostazioni globali e console**. Selezionare **Amministra** in **Console**, come mostrato nell'immagine.

≡	nexpose' Create 🗸				۵	54	@~	đ	۹	e admin	~
ô											
88	2 Liers	Asset Groups	P2 Exceptions and Overrides		m e	lendar					
Q	Create and manage user accounts or manage custom user roles	Create dynamic or static asset groups and manage existing asset	Review requests to exclude vulnera	bilities from reports and to	View ca	lendar of all	scheduled sca	ns, blackouts	, database (operations	
受	and password policy.	groups.	override policy compliance results.		and rep	orts.					
Ø					_						
R	⊗ Scan Options										
ø	ENGINES Create and manage available Scan Ex	ingines, and Scan Engine Pools.	HISTORY	View current and past scans for this	installation.						
	SHARED CREDENTIALS Create and manage shared credentia	als for authenticated scans.	TEMPLATES	Create and manage scan templates	for controlling	g and tuning	scans.				
Ø	BLACKOUTS Create and manage global blackout s	settings.	ROOT CERTIFICATES	Manage root certificates used in sca	nning and wa	irehouse exp	port.				
⊨											
	Q. Discovery Options		Global and Console Settings								
	NSX MANAGER Create and manage settings that give the NSX OVF distribution.	a Scan Engine direct access to an NSX network of virtual assets.Update	GLOBAL	Manage global settings for selecting Administer set ings for the Security	risk score st Console, inch	rategies and uding auto-u	l excluding assi	ets from scar	15.		
	CONNECTIONS Create and manage connections that	allow the Security Console to discover assets dynamically.	00110022			ang aato a	pager 6.19.1933	ng secongs.			
	EVENTS View events and statistics for asset di	liscovery mechanisms.									

Fare clic su Gestisci certificato, come illustrato nell'immagine:

≡	nexpose Create		
仑			
	Security Console Con	figuration	
Ţ			
4	GENERAL	The Security Console contains an embedde	d web server. The following web server settings can be configured.
愛	UPDATES	WEB SERVER SETTINGS	
\oslash		Web server port	j3780
	WEB SERVER	Session timeout (seconds)	600
×	PROXY SETTINGS	Jession inteour (seconds)	000
Ø		Initial request handler threads	10
_	AUTHENTICATION	Maximum request handler threads	100
Ø			
	DATABASE	Failed login threshold	4
	SCAN ENGINES	HTTPS certificate	Issued to nexpose.example.com
	LICENSING		Valid until Thu Nov 22 01:16:44 PST 2018
	EXPOSURE ANALYTICS		MANAGE CERTIFICATE

Come mostrato nell'immagine, fare clic su in **Crea nuovo certificato**. Immettere il **Nome comune** ed eventuali altri dati che si desidera includere nel certificato di identità di Nexpose Scanner. Verificare che ISE sia in grado di risolvere l'FQDN dello scanner Nexpose con DNS.

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 (fully 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	

Esportare la richiesta di firma del certificato (CSR) nel terminale.



A questo punto è necessario firmare il CSR con CA (Certification Authority).

The Security Console the CSR below and se Security Console usin	has generated a certificate nd it to your CA for signate o the 'Import Signed Certif	e signing request fo ure. The signed cert ficate' button.	r the current certificate. Yo ificate can later be importe	ou may copy ed into the
BEGIN NEW CERTIF MIIEYzCCAksCAQAwH DQYJKoZIhvcNAQEBB oyg3oC9MeML7s1Tug GB+Sq4bAfqHFIKIsjdn q4qc9DH6RuYUOEYaw mwJFNG13BILZykhjM rsay1voSprJXjncC3xA JEQpzLxjQsnAZRG8dy S0WExoXpWL8oZbOtF j84GMbFuYvBq+x08pr w/oD2cQFCdp1XBC7c OeNlx41XDaudLii/SuY	ICATE REQUEST IJECMBoGA1UEAxMTbmV4c QADggIPADCCAgoCggIBAIM D0K4pvmIZOh1E+B6bK7ZO j3eOOLW7h8TPmD57NOZO vclWs+7wTVRDt+hyFL6v6e6 zZVsnnGWAn9IghqQRNftXW XHWQGFknY8d8eoaEM82fU 9+J52S6Zm7RXyCg0p7MRH 2HheWaQSmPStzeuQpiFXNj U/kGEVftVABGHnjnstGN+qI UdvkXMIJwqQXtpd8uz9ZLv BB03DLbN6Inu7Vp+5/3W59	G9zZS5leGFtcGxlLm VOylrdSOlrDwLMaHEl B3QAnf9/VxKaur/Q/y v4X8v6DOz42YF8TNS ireIXF7NIp8ssqC02Zv V5JHYdFVs84WeB+DI Jdzz6Y/jOqUH6ToZ5rr KlykEOMGEqR5TFOZV th/XQ0gHpc48v+1Dd M8CU93mq/6NNPmz K+afJT8cBphledh1Fy PlcfmHlt+3oEJAnWx2	NvbTCCAilw SqHZoG4G CNj1AcYH ImScbeTZ5 DGzLnzb KX1KWneigL hEAsKINg VCfTxomvzp DeZI/wrLd 8XCgAxCOm +v7Mu+m vVCLgD	

Importare il certificato rilasciato dalla CA facendo clic su Importa certificato.

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.

Configurare un sito. Il sito contiene risorse che è possibile analizzare e l'account utilizzato per integrare ISE con Nexpose Scanner deve disporre dei privilegi per gestire i siti e creare i report. Passare a **Crea > Sito**, come mostrato nell'immagine.

CLOSE

≡	nexpose	Create 🔨
仚		Asset Group
		Dynamic Asset Group
		Report
_	0	Site
Ţ	0	Tags

Come mostrato nell'immagine, immettere il **Nome** del Sito nella scheda **Info & Security**. La scheda **Assets** deve contenere gli indirizzi IP delle risorse valide, gli endpoint idonei per l'analisi delle vulnerabilità.

≡	nexpose	Create 🗸					_	■ %	ද [ී]
	Site Co	onfiguration							SAVE & SCAN SAVE CANCEL
						•			
		INFO & SECURITY	ASSETS	AUTHENTICATION	TEMPLATES	Ö ENGINES		ALERTS	SCHEDULE
	GENERAL		General						
	ORGANIZ	ATION		Name AAA TAC		~			
	ACCESS			Importance Normal		v			
				Description					
									ĥ
			User-added Tags CUSTOM TAGS	LOCA	ATIONS	OWNERS		CRITICALITY	
			None	N	one	None		None	Add tags
	nexpose'	Create						■ % ©~	ດີ Q 2 admin
	Site C	onfiguration							SAVE & SCAN SAVE CANCEL
Q		INFO & SECURITY	Ģ			%		Ø	ä
			ASSETS	AUTHENTICATION	TEMPLATES	ENGINES		ALERTS	SCHEDULE
0	Specify	assets by Names/Addres	ses Connection						
ç	INC	UDE				1 assets 🗸	EXCL	JDE	0 assets 🗸
	1	Assets Browse No	file selected.				0	Assets Browse No file selected.	
		10.229.20.32 × Enter name	e, address, or range.					Enter name, address, or range.	
						÷			

Importare il certificato CA che ha firmato il certificato ISE nell'archivio protetto. Selezionare Amministrazione > Certificati radice > Gestisci > Importa certificati.

≡	nexpose	Create V	8	52	@~	\$ Q	ိ admin
							\bigcirc tems \lor
					-		
		SUSTOM CERTIFICATES 🛛 🖗					^ ×
		IMPORT CERTURATES					
		Distinguished Name	SHA-1 Fingerprint			Expires On	Delete
		CN+LAB CA, DC-example, DC-com	FD729A388533726FF8450	358A2F7EB27I	C8A1178	02/12/2025	Ē
R							
	,	RESET CERTIFICATES 💿					
		Distinguished Name	SHA-1 Fingerprint			Expires On	
		CN-DigiDert Assured ID Root CA, OU-www.digicert.com, 0+DigiDert Inc, C+US	056388630D62D75A88C8	AB1E48DF85A	99824043	11/10/2031	
		CN-TG TrustCenter Class 2 CA II, OU-TC TrustCenter Class 2 CA, O-TC TrustCenter GmbH, C+DE	AE5083ED7CF45CBC8F61	C621FE685D79	4221156E	12/31/2025	
		EMAILADDRESS-premium-server@thavte.com, CN=Thavte Premium Server CA, OU-Dertification Services Division, O=Thavte Consulting cc, L=Cape Town, ST=Western Cape, O=ZA	E0AB05942072549305606	2023670F7CD2	EFC6666	01/02/2021	

Configurare ISE

Passaggio 1. Abilitare i servizi TC-NAC.

Abilitare i servizi TC-NAC sul nodo ISE. Tenere presente quanto segue:

- Il servizio NAC incentrato sulle minacce richiede una licenza Apex.
- Ènecessario un PSN (Policy Service Node) distinto per il servizio NAC incentrato sulle minacce.
- Il servizio NAC incentrato sulle minacce può essere abilitato solo su un nodo in una distribuzione.

• Èpossibile aggiungere una sola istanza di una scheda per fornitore per il servizio di valutazione delle vulnerabilità.

cisco Identi	ty Services I	Engine	Home 🔸	Context Visibility	 Operations 	Policy	 Administration 	Work Centers
▼System	Identity Mail	nagement 🕨	Network Res	sources • Device	Portal Managem	ent pxGrid Se	vices Feed Sen	vice
Deployment	Licensing	Certificates	Loggin	g Maintenanc	e Upgrade E	Backup & Restore	Admin Access	► Settings
Deploym	ent		₩ .	Deployment Nod Edit Node General Setti	es List > ISE22-1 0 ngs Profilin	ek g Configuration		
• कुछ 06 कुछ PA	N Failover				Hostname ISI FQDN ISI IP Address 10 Node Type Ide	E22-1ek E22-1ek.examp .48.23.86 entity Services	le.com Engine (ISE)	
				Personas				
				Administrat	on		Role STANDA	ALONE Make Primary
				Monitoring			Role	ARY
				Policy Servi	ce			
				🗹 En	able Session Servi	Personas ces	Include Node	in Node Group None T
				✓ En	able Profiling Serv	rice		
				🗹 En	able Threat Centri	ic NAC Service		
				🗆 En	able SXP Service	(i)	Use Interface	GigabitEthernet 0 +
				🗆 En	able Device Admir	n Service		
				□ _{En}	able Passive Ident	ity Service		
				□ pxGrid	Ð			

Passaggio 2. Importare il certificato dello scanner Nexpose.

Importare il certificato CA dello scanner Nexpose nell'archivio Certificati attendibili di Cisco ISE (Amministrazione > Certificati > Gestione certificati > Certificati attendibili > Importa). Verificare che i certificati radice e intermedi appropriati siano importati (o presenti) nell'archivio dei certificati protetti di Cisco ISE

dentity Services Engine	Home Context Visibility Operations Police	y • Administra	ation Work Centers						Licens
System Identity Management Deployment Licensing Certificate	Network Resources Device Portal Management pxGr es Logging Maintenance Upgrade Backup & Re	id Services → Fe store → Admin /	eed Service	tric NAC					Click here to do wireless setu
0									
- Certificate Management	Trusted Certificates								
System Certificates	/ Edit 💠 Import 😨 Export 🗙 Delete 🔎 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	V
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	~
	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	2
	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	

Passaggio 3. Configurare l'istanza TC-NAC di Nexpose Scanner.

Aggiungere Rapid7 Instance in Administration > Threat Centric NAC > Vendor di terze parti.

dentity Servi	ces Engine	Home	Context	Visibility	• Operations	Policy	▼ Adm	inistration	► W	/ork Centers
System Identit	y Management	Network	Resources	Device	Portal Management	pxGrid S	ervices	Feed Ser	vice	Threat Centric NAC
Third Party Vendors										
Vendor Instances > N Input fields marked w	New vith an asterisk (*)	are required	1.							
Ve	ndor * Rapid7	Nexpose : \	/A				•			
Instance N	lame * Rapid	7								
					C	ancel	ave			

Una volta aggiunta, l'istanza passa allo stato **Pronta per la configurazione**. Fare clic su questo collegamento. Configurare **Nexpose Host** (Scanner) e **Port**. Per impostazione predefinita, il valore è 3780. Specificare **Nome utente** e **Password** con accesso al sito corretto.

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.	
Username to access Nexpose Security Console.	
Username to access Nexpose Security Console.	
Username to access Nexpose Security Console. Password	
Username to access Nexpose Security Console. Password Password of the user.	
Username to access Nexpose Security Console. Password Password of the user.	
Username to access Nexpose Security Console. Password Password of the user. Http proxy Host	
Username to access Nexpose Security Console. Password Password of the user. Http proxy Host	
Username to access Nexpose Security Console. Password Password of the user. Http proxy Host Optional http proxy host. Requires proxy port also to be set.	
Username to access Nexpose Security Console. Password Password of the user. Http proxy Host Optional http proxy host. Requires proxy port also to be set.	
Username to access Nexpose Security Console. Password Password of the user. Http proxy Host Optional http proxy host. Requires proxy port also to be set. Http proxy port	

Cancel

Next

Le impostazioni avanzate sono ben documentate nella Guida dell'amministratore di ISE 2.2. Il link è disponibile nella sezione Riferimenti di questo documento. Fare clic su **Avanti** e **Fine**. Nexpose Instance passa allo stato **Attivo** e viene avviato il download della Knowledge Base.

dentity Services I	Engine Home	Context Visibility	Operations	Policy Administration	Work Centers	
System Identity Mar	nagement Network R	Resources	Portal Management	pxGrid Services Feed Se	Threat Centric NAC	
Third Party Vendors						
Vendor Instances	m Trash ▼ 🕑 Eo	dit Restart Stop)		▼ Filter ▼	¢-
Instance Name	Vendor Name	Туре	Hostname	Conn	ectivity Status	
Rapid7	Rapid7 Nexpos	e VA	nexpose.exa	mple.com Conne	ected Active	

Passaggio 4. Configurare il profilo di autorizzazione per attivare la scansione VA.

Passare a **Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione**. Aggiungi nuovo profilo. In **Operazioni comuni** selezionare la casella di controllo **Valutazione vulnerabilità**. L'intervallo di scansione su richiesta deve essere selezionato in base alla progettazione della rete.

Il profilo di autorizzazione contiene le seguenti coppie av:

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

Vengono inviati ai dispositivi di rete all'interno di un pacchetto di accettazione dell'accesso, anche se il loro vero scopo è quello di dire al nodo MNT (Monitoring) che deve essere attivata la scansione. MNT indica al nodo TC-NAC di comunicare con Nexpose Scanner.

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
Authorization Profiles	Network Device Profile dds Cisco 👻 🕀
Downloadable ACLs	Service Template
▶ Profiling	
▶ Posture	Passive Identity Tracking i
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 Image: Select an item Image: Select an item Access Type = ACCESS_ACCEPT Cisco-av-pair = on-demad-scan-interval=48 Cisco-av-pair = va-adapter-instance =c2175761-0e2b-4753-b2d6-9a9526d85c0c

Passaggio 5. Configurare i criteri di autorizzazione.

- Configurare il criterio di autorizzazione per utilizzare il nuovo profilo di autorizzazione configurato nel passaggio 4. Passare a Criterio > Autorizzazione > Criterio di autorizzazione, individuare la regola Basic_Authenticated_Access e fare clic su Modifica. Modificare le autorizzazioni da PermitAccess al nuovo Standard Rapid7 creato. In questo modo viene eseguita una scansione delle vulnerabilità per tutti gli utenti. Fare clic su in Salva.
- Crea criteri di autorizzazione per computer in quarantena. Passare a Criterio > Autorizzazione
 > Criterio di autorizzazione > Eccezioni e creare una regola di eccezione. Passare quindi a Condizioni > Crea nuova condizione (opzione avanzata) > Seleziona attributo, scorrere verso il basso e selezionare Minaccia. Espandere l'attributo Threat e selezionare Nexpose-CVSS_Base_Score. Modificare l'operatore in Maggiore di e immettere un valore in base ai criteri di sicurezza. Il profilo di autorizzazione della quarantena deve consentire un accesso limitato alla macchina vulnerabile.

dent	ty Services Engine Home	Context Visibility Operations Policy Administration Work	x Centers	License Warning 🔺 🔍 😑 🔿 Ö
Global Exce	ptions Policy Authentication Authorit	zation Profiling Posture Client Provisioning Policy Elements		Click here to do wireless setup and visibility setup Do not show this again.
Authorizat Define the Au For Policy Exp First Matcher	ion Policy horization Policy by configuring rules base of go to Administration > System > Backu Rule Applies v	d on identity groups and/or other conditions. Drag and drop rules to change the order ρ & Restore $>$ Policy Export Page		
▼ Excepti	ons (1)			
i 🔽	Exception Rule	Conditions (identity groups and other conditions) Threat Baold7 Nexpose-CVSS, Base, Score GREATER 1	then Quarantine	Edd -
Standard				
Ciab	Bule Name	Conditions (identity envire and allow conditions)	Barmiasiana	
	Wireless Black List Default	If Blacklist AND Wireless_Access	then Blackhole_Wireless_Access	Edtiv
	Profiled Cisco IP Phones	If Cisco-IP-Phone	then Cisco_IP_Phones	Edt •
	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones	Editiv
0	Compliant_Devices_Access	If (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess	Edt I 🗸
0	Employee_EAP-TLS	If (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD	Edit I 🕶
0	Employee_Onboarding	If (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD	Editiv
	Wired_Guest_Access	If (Guest_Flow AND Wired_MAB)	then PermitAccess AND Guests	Edt I 🕶
	Wi-Fi_Guest_Access	If (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests	Editiv
	Wired_Redirect_to_Guest_Login	If Wired_MAB	then Cisco_WebAuth	Edt i 🕶
	Wi-Fi_Redirect_to_Guest_Login	If Wireless_MAB	then Cisco_WebAuth	Edit i 🕶
	Basic_Authenticated_Access	If Network_Access_Authentication_Passed	then Rapid7	Edit I 🕶
	Default	If no matches, then DenyAccess		Edt I 🕶

Verifica

Identity Services Engine

La prima connessione attiva VA Scan. Al termine dell'analisi, la riautenticazione CoA viene attivata per applicare nuovi criteri, se corrispondenti.

diale Ident	ity Services Engine	Home Conte	xt Visibility	* Operations	Policy Administration	on							Licens	e Warning 🔺 🔍 🔍	0 0	o
▼RADIUS	Threat-Centric NAC Live	Logs + TACACS	Troubleshood	t Adaptive	Network Control Reports							Click b	ere to do wireless setu	and visibility setup D	not show this again.	×
Live Logs	Live Sessions															
		Misconfigured Su	pplicants O		Misconfigured Network I	Devices (0	RADIUS Drops	0	CI	lient Stopped Responding 0		Rep	eat Counter 0			
		0			0		0			0			0			
										Refrest	Every 1 minute	• Sh	ow Latest 20 reco	rds • Within	Last 24 hours	•
C Refresh	Reset Repeat Count	ts 💆 Export To 🕶													▼ Filter • C	••
Time		Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authenticat	Authorizati	Authorization Profiles	IP Address		Network Device	Device Port	Identity Group	
×		Status			Identity	Endpoint ID	Endpoint Prof	Authentication	Authorization	Authorization Profiles	IP Address	-	Network Device	Device Port	Identity Group	
Nov 2	4, 2016 01:45:41.438 PM	0	0	0	alice	3C:97:0E:52:3F:D9	Nortel-Device	Default >> D	Default >> E	Quarantine	10.229.20.32			FastEthernet1/0/5		
Nov 2	4, 2016 01:45:40.711 PM	~	0		alice	3C:97:0E:52:3F:D9	Nortel-Device	Default >> D	Default >> E	Quarantine	10.229.20.32		Switch_2960	FastEthernet1/0/5	Profiled	
Nov 2	4, 2016 01:45:39.166 PM	~	0			3C:97:0E:52:3F:D9							Switch_2960			
Nov 2	4, 2016 01:32:00.564 PM		0		alice	3C:97:0E:52:3F:D9		Default >> D	Default >> B	Rapid7	10.229.20.32		Switch_2960	FastEthernet1/0/5		

Per verificare quali vulnerabilità sono state rilevate, selezionare **Context Visibility > Endpoints**. Verificare le vulnerabilità degli endpoint con i punteggi assegnati dallo scanner Nexpose.

cisco Identity S	Services Engine Home	▼ Context Visibility	 Operations 	Policy	Administration	Work Centers
Endpoints U	sers Network Devices					
Endpoints > 3	C:97:0E:52:3F:D9					
3C:97:0E	:52:3F:D9 ØØ	8				
	MAC Address: 3C:97:0E:52:3I Username: alice Endpoint Profile: Nortel-Devic Current IP Address: 10.229.20 Location: Location -> All Loca	F:D9 e .32 ations				
Appli	cations Attributes	Authentication TI	hreats Vuln	erabilities		
ssl-cve-2016	2183-sweet32					
Title:	TLS/SSL Birthday attacks on 64	4-bit block ciphers (SWEE	ET32)			
CVSS score:	5					
CVEIDS:	CVE-2016-2183					
Reported by:	Rapid7 Nexpose					
Reported at:	Thu Nov 24 05:42:52 CET 2016	6				
ssl-static-key	r-ciphers					
Title:	TLS/SSL Server Supports The	Use of Static Key Ciphers	3			
CVSS score:	2.5999999					
CVEIDS:						
Reported by:	Rapid7 Nexpose					
Reported at:	Thu Nov 24 05:42:52 CET 2016	6				
rc4-cve-2013	-2566					
Title:	TLS/SSL Server Supports RC4	Cipher Algorithms (CVE-	2013-2566)			
CVSS score:	4.30000019					
CVEIDS:	CVE-2013-2566					
Reported by:	Rapid7 Nexpose					
Reported at:	Thu Nov 24 05:42:52 CET 2016	6				

In Operazioni > TC-NAC Live Logs, è possibile visualizzare i criteri di autorizzazione applicati e i dettagli su CVSS_Base_Score.

dentity Services Engine Home	Context Visibility Operat	ions Policy	Administration	Work Center				License Warning 🔺 🌼		• •	
RADIUS Threat-Centric NAC Live Logs T	ACACS + Troubleshoot + Ac	laptive Network Contro	Reports					Click here to do wireless setup and visibility setup D	to not show this	s again.	
Threat Centric NAC Livelog											
C Refresh 💆 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			

Scanner Nexpose

Quando l'analisi VA viene attivata da TC-NAC Nexpose Scan, le transizioni allo stato **In corso** e lo scanner inizia a eseguire il probe dell'endpoint. Se si esegue l'acquisizione wireshark sull'endpoint, a questo punto si verificherà lo scambio di pacchetti tra l'endpoint e lo scanner. Al termine dell'esecuzione dello scanner, i risultati saranno disponibili nella **home page**.

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

Nella pagina **Asset**, è possibile verificare la presenza di un nuovo endpoint con i risultati dell'analisi, l'identificazione del sistema operativo e il rilevamento di 10 vulnerabilità.



Quando si fa clic sull'**indirizzo IP dell'endpoint,** Nexpose Scanner visualizza il nuovo menu, in cui è possibile visualizzare ulteriori informazioni, tra cui nome host, punteggio Risc e elenco dettagliato delle vulnerabilità

=	nexpo	ose'	Create 🗸									Ş∧.	⊙~ ¢	ુ વ	ු a	lmin
ô																TEMS $^{\sim}$
88		TAC 444 1	Manual alter													
0		ino non i	1.000													
		ADDR	ESSES 10.22	29.20.32	OS	Kicrosoft Windows	RISH	SCORE 😡			US	ER-ADDED TA	GS 🕢			
쓪		HARD	WARE Unkn	own	CPE		C	RIGINAL		CUSTOM TAGS			OWNE	ERS		
Ø		ALIAS	ES TAC-	PC	LAST SCAN	Nov 24, 2016 4:42:07 AM (6 minutes ago)	2	2,016		None			Nor	16		
Q		HOST	TYPE Unkn	own	NEXT SCAN	Not set	CONT	EXT-DRIVEN							Add	ags
_		IDENT	JE IFIERS				2	2,016		LOCATIONS None			CRITIC/ Nor	ie		
L		SITE	TAC	AAA												
Ø		SCAN	ASSET NOW	CREATE ASSET REPORT DELETE ASSET	SEND LOG											
⊨		_														
=	nexpos	se' (Create 🗸								6			~ .		
												74		ч [•]		admin
~												74	@¢	Ų	~ õ	admin
Û		VULNER	ABILITIES									74	<i>(</i>)•	Ļ		admin
心 器	Г	VULNER View detail	ABILITIES	i vulnerabilities. To use one of the exception controls	on a vulnerability, se	lect a row. To use the control with all displayed displayed vulnerations are the solution of model.	ibilities, select the top rc	w and use Selec	rt Visible. Ca	ncel all selections using Clear All. €	,	γ _Α	00	-	ă ă	admin
	ľ	VULNER View detail Exposures	ABILITIES Is about discovered : 🔗 Susceptible 1	d vulnerabilities. To use one of the exception controls o mahvare attacks 🖗 Metasploit-exploitable 🚯 Vi	on a vulnerability, se alidated with Metasp	lect a row. To use the control with all displayed displayed vulneral for $\underline{\mathcal{X}}$ Explore published explore	abilities, select the top ro	w and use Selec	rt Visible. Ca	ncel all selections using Clear All. 🍯)	γ		Ų		admin
	ſ	VULNER View detail Exposures EXCLI	ABILITIES Is about discovered : 🔮 Susceptible 1 UDE RECALL	é vulnerabilites. To use one of the exception controls o malware attacks @ Metasplot exploitable @ V . RESUBMIT	on a vulnerability, se alidated with Metasp	lect a row. To use the control with all displayed displayed withered for T. Explort published 🚯 Validated with published explort	abilities, select the top ro	w and use Selec	rt Visible. Ca	ncel all selections using Clear All. 🍯	, ,	ŶA.	То	tal Winerabili	ies Selected: 0	admin
○ 器 ◆		VULNER View detail Exposures: EXCLU	ABILITIES Is about discovered Susceptible 1 UDE RECALL RECALL	é vulnerabilites. To use one of the exception controls o malware attacks @ Metasplot exploitable @ vi . RESUBMIT	i on a vulnerability, se alidated with Metasp	lect a row. To use the control with all displayed displayed values to the ${\bf X}$ Explorit published ${\bf X}$ Validated with published explorit	oblities, select the top ro	w and use Selec	t Visible. Ca CVSS	ncei all selections using Clear All. @ Risk Published Or	. Mo	γA dified On	To Severity v	tal Vulnerabilit Instances	ies Selected: 0 Exceptions	of 10
		VULNER View detail Exposures Excu	ABILITIES is about discovered Susceptible 1 UDE RECALL inte LS/SSL Birthday at	d vulnerabilities. To use one of the exception controls o malware attacks @ Metasplok exploitable @ v . RESUBMIT tacks on 64-bb block ciphers (IWEET32)	i on a vulnerability, se alidated with Metasp	lect a row. To use the control with all displayed displayed vulneral loct 🚡 Explori published 🚯 Validated with published explori	shifties, select the top rc	w and use Selec	rt Visible. Ca CVSS	ncel all selections using Clear Al. @ Risk Published Or 5 425 Wed Aug 24	Mo 2016 Fri	tified On Sep 02 2016	To Severity ~ Severe	tal Vulnerabilit Instances	ies Selected: 0 Exceptions 1 2 Exclude	of 10
		VULNER View detail Exposures ExCLU	ABILITIES Is about discovere Susceptible 1 UDE RECALL itle LS/SSL Birthday at LS Server Supports	d vulnerabilities. To use one of the exception controls to malware attacks @ Metasploit exploitable @ V . RESUBMIT tacks on 64-bit Mock ciphers (SWEET32) 1TLS version 1.0	i on a vulnerability, se alidated with Metasp	lect a row. To use the control with all displayed displayed witheral lot. 🗼 Exploit published 🐴 Validated with published exploit	abilities, select the top ro	w and use Selec	cvss	Risk Published Or 5 425 Wed Aug 24 3 324 Two Oct 14 12	Mo- 2016 Fri 1 014 Thu	24 dified On Sep 02 2016 I Nov 12 2015	To Severity ~ Severe Severe	tal Wuhersbill Instances	ies Selected: 0 Exceptions 1 2 Exclude 1 2 Exclude	of 10
℃ 器 ♥ ♥ ②		VULNER View detail Exposures: ExCU	ABILITIES is about discovered Susceptible 1 UDE RECALL inte LS/SSL Birthday at LS/SSL Server Support LS/SSL Server Support	Vulnersbilltes. To use one of the exception controls o malware attacks W Metasplot explorable W V RESUBMIT tacks on 64-bit block ciphers (IVVEET32) ITLS version 1.0 ports RC4 Cipher Algorithms (IVV20132566) ports RC4 Cipher Starts	i on a vulnerability, se alidated with Metasp	Nect a row. To use the control with all displayed displayed vulneral lot. 🚡 Exploit published 🐴 Validated with published exploit	abilities, select the top ro	w and use Selec	cvss	Risk Published Or 5 425 Wed Aug 24 3 324 Tue Oct 14 2 3 497 Tue Mort 14 3 497 Tue Mort 14	Mo 2016 Fri 1 014 Thu 013 Thu	4/16/2016 Sep 02 2016 Nov 12 2015 Apr 28 2016	To Severity - Severe Severe Severe Severe	tal Winerabili	les Selected: 0 Exceptions 1 @ Exclude 1 @ Exclude 1 @ Exclude	of 10
		VULNER View detail Exposures: EXCLU T T T	ABILITIES Is about discovered Susceptible 1 UDE RECALL RECALL IS Server Support: LS/SSL Birthday at LS/SSL Server Sup LS/SSL Server is e 15/SSL Server is e	f vulnerabilities. To use one of the exception controls or malware attacks @ Metasploit-exploitable @ V . EESUBMIT tacks on 64-bit block ciphers (IVEET32) > TLS version 1.0 ports RO4 Cipher Algorithms (IVE 2013-2564) making the EACT attack cipher Careford (Data backster)	i on a vulnerability, se alidated with Metasp	Rect a row. To use the control with all displayed displayed vulneral lot. 🚡 Exploit published 💑 Validated with published exploit	abilities, select the top ro	w and use Select	cvss	Risk Published Or 5 425 Wed Aug 24 3 324 Tue Oct 14 2 3 397 Tue Mar 12: 3 448 Tue Set 14:	Mo 2016 Fri 1 014 Thu 013 Thu 011 Thu	dified On Sep 02 2016 I Nov 12 2015 I Apr 28 2016	To Severity - Severe Severe Severe Severe	tel Vulnersbill Instances	les Selected: 0 Exceptions 1 © Exclude 1 © Exclude 1 © Exclude 1 © Exclude	of 10
℃ 88 ♦ 0 23		VULNER View detail Exposures: CCLU T T T T	ABILITIES is about discovered Susceptible to RECALL UDE RECALL UDE RECALL LS/SSL Server Support LS/SSL Server Support LS/SSL Server is U LS/SSL Server is U	Vulnerabilities. To use one of the exception controls or malware attacks @ Metasploit-exploitable @ V . <u>RESUBNIT</u> tacks on 64-bit block ciphers (IVVECT32) a TL3 version 1.0 ports RC4 Cipher Algorithms (IVVE 013-2566) making the EEACT attack aim Commonly Used Prime Numbers	i on a vulnerability, se alidated with Metasp	lect a row. To use the control with all displayed displayed vulneral for 3. Explore published in Validated with published explore	bilities, select the top ro	w and use Selec	tt Visible. Ca	Risk Published Dr. 5 425 Wed Aug 24 3 324 Tue Oct 142 3 397 Tue Mar 12; 4 Tue Step 65; 91.0 Wed Mar 22; 6 91.0 Wed Mar 24; 100	Mo 2016 Fri 1 014 Thu 013 Thu 011 Thu 2015 Thu	dified On Sep 02 2016 I Nov 12 2015 I Apr 28 2016 I Feb 18 2016 Jun 16 2016	To Severity - Severe Severe Severe Severe Moderate	tal Vulnerabili Instances	Ins Selected: 0 Exceptions 1 © Exclude 1 © Exclude 1 © Exclude 1 © Exclude 1 © Exclude	of 10
		VULNER View detail Exposures: EXCLU T T T T T T	ABILITIES is about discoverer Susceptible to RECALI UDE RECALI RIC LL/SSL Birthday at LS/SSL Server Support LS/SSL Server Support	Vulnerabilities. To use one of the exception controls on malware attacks @ Metasploit-exploitable @ V . RESUBNIT tacks on 64-bit Mick Ciphers (SWEET32) . TLS version 1.0 ports RC4 Cipher Algorithms (CVE-2013-2566) making the BEAGT attack atting Commonly Liad Prime Numbers samaller than 2048 bits	i on a vulnerability, se	lect a row. To use the control with all displayed displayed vulneral to the second second with all displayed with published exploit for a second seco	abilities, select the top ro	w and use Selec	CVSS 43 43 43 20 20	Risk Published 00 425 Wed Aug 24 3 327 Tue Dict 14 2 3 397 Tue Mar 12 3 4 Tue Sep 65 2 91.0 Wed May 20 5 91.0 Wed May 20 5 6 91.0 Wed May 20 5	Mo 2016 Fri 014 Thu 013 Thu 011 Thu 2015 Thu 2015 Thu	24 dified On Sep 02 2016 i Nov 12 2015 i Apr 28 2016 i Feb 18 2016 i Jun 16 2016 i Nov 12 2015 i Apr 2015	To Severity ~ Severe Severe Severe Severe Moderate Moderate	tal Vulnerabili Instances	les Selected: 0 Exceptions 1 @ Exclude 1 @ Exclude 1 @ Exclude 1 @ Exclude 1 @ Exclude 1 @ Exclude 1 @ Exclude	of 10
		VULNER View detail Exposures: EXCLU	ABILITIES is about discovere Susceptible to RECALI UDE RECALI RIC LS/SSL Birthday at LS/SSL Server Support LS/SSL Server Sup Office Heliman group LS/SSL Server Sup	Vulnersbillies. To use one of the exception controls on malware attacks @ Metaspion exploitable @ W . RESUBNT tacks on 64-bit block ciphers (SWEET32) TLT aversion 1.0 ports RC4 Cipher Agenthms (SVE 2013 2566) making the BEAST attack step Commonly Lited Prime Numbers smaller than 2548 bits ports The Use of Static Kky Ciphers come	ion a vulnerability, se	fect a row. To use the control with all displayed displayed witheral for T Explor published in Validated with published explort	abilities, select the top ro	w and use Select	cvss cvss 43 43 20 20 20	Risk Published Or 5 425 Wed Aug 24 0 324 Tue Oct 142 0 377 Tue Mar 122 0 448 Tue Sop 65 5 91.0 Wed May 20 6 91.0 Wed May 20 5 91.0 Wed May 20 5 91.0 Wed May 20 0 0,0 F(A-m0 11)	Mo 2016 Fri 2014 Thu 013 Thu 2015 Thu 2015 Thu 2015 Thu 2015 Thu	24 dified On Sep 02 2016 I Nov 12 2015 I Apr 28 2016 I Feb 18 2016 I Jun 16 2016 I Nov 12 2015 d Sep 30 2015 Jul 12 2012	To Severity ~ Severe Severe Severe Moderate Moderate Moderate	tal Vulnerabili Instances	es Selected: 0 Exceptions Deceptions Decepti	of 10
C ::::		VULNER View detail Exposures: EXCLU C+ T T T T T T T T T T T T T T T T T T	ABILITIES is about discoverse Susceptible 1 is is LS/SL Birthday at LS/SL Berver Support LS/SL Server is LS/SL Server	Vulnersbillies. To use one of the exception controls or malware attacks @ Metasploit exploitable @ W . RESUBATT tacks on 64-bit block ciphers (SWEET22) TLS version 1.0 opris RO4 Cipher Agonthms (CVE-2013-256A) mabling the BEAST attack asing Commonly Used Prime Numbers or maliet than 2546 bits ports The Use of Static Kay Ciphers comme	on a vulnerability, se	lect a now. To use the control with all displayed displayed witheral for $\underline{\mathcal{X}}$ Explort published $\widehat{}$ Validated with published explort	abilities, select the top ro	w and use Selec	cvss cvss 43 43 21 21 21	Risk Published OF 5 425 Wed Aug 24 6 324 Tue On C1 142 3 324 Tue On C1 142 4 Tue Sep 65 91.0 5 91.0 Wed May 20 6 91.0 Wed May 20 5 240 Sun Feb 01 2 0.0 Fri Aug 01 11 0 0.0 Sun Feb 01	Mo 2016 Fri 314 Thu 013 Thu 2015 Thu 2015 Thu 2015 Thu 2015 Thu 2015 Thu 2015 Thu 2015 Thu 2014 We	24 dified On Sep 02 2016 i Nov 12 2015 i Apr 28 2016 i Apr 28 2016 i Jun 16 2016 i Jun 16 2016 d Sep 30 2015 i Jul 12 2012 d Dec 10 2014	To Severity - Severe Severe Severe Severe Moderate Moderate	tal Vulnersbill Instances	les Selected: 0 Exceptions 1 © Exclude 1 © Exclude	of 10
C Image: Second sec		VULNER View detail Exposures: EXCLU T T T T T T T T T T T T T	ABILITIES is about discoverse Susceptible 1 is about discoverse Susceptible 1 Re LS/SL Strickly at LS/SL Server Sup LS/SL Server Sup LS/SL Server Sup LS/SL Server Sup LS/SL Server Sup CP timetary res DP SDP Traffic / LS/SL Server Sup	Vulnersbilltes. To use one of the exception controls on makers attacks @ Metasplot.explotable @ V RESUBUT tacks on 64-bit block ciphers (SWEET22) TLS version 1.0 TLS version 1.0 TLS version 1.0 ports RPC Cipher Algorithms (CVE-2013-2564) sing Commonly Used Prime Numbers ports The Use of Static Key Ciphers ports The Use of Static Key Ciphers ports The Use of Static Key Ciphers ports 2015 October Suite	on a vulnenbilly, se alidated with Metasp	iect a row. To use the control with all displayed displayed withered for The Deplot published with published exploit.	abilities, select the top ro	w and use Selec	cvss 43 43 43 21 21 21	Incel all selections using Clear All. Resk Published OF 5 425 Wed Aug 24 a 324 Tuo Oct 142 a 3247 Tuo Oct 142 a 3247 Tuo Oct 142 a 348 Tuo Sep 66 a 91.0 Wed May 20 a 240 Sun Feb 01 a 0.0 Fri Aug 011 a 0.0 Sun Feb 01 a 0.0 Sun Feb 01 a 0.0 Sun Feb 01	Mo 2016 Fri 1 014 Thu 013 Thu 2015 Thu 2015 Thu 2015 Thu 1015 We 197 Thu 1014 We	24 dified On Sep 02 2016 i Nov 12 2015 i Apr 28 2016 i Apr 28 2016 i Apr 28 2016 i Jun 16 2016 i Nov 12 2015 d Sep 30 2015 i Jul 12 2012 d Dec 10 2014 n Feb 15 2016	To Severity - Severe Severe Severe Severe Moderate Moderate Moderate Moderate	tel Vulnerabili Instances	les Selected: 0 Exceptions 1 © Exclude 1	of 10

Quando si fa clic su nella **Vulnerabilità** stessa, nell'immagine viene visualizzata una descrizione completa.

	nexpo	ose	Create 🗸											đ		🖄 admin
																-
			VULNERABILITY INFOR	MATION												
			OVERVIEW													
			Title						Severity	Vulnerability ID	CVSS		F	Published	Modified	
Q			TLS/SSL Birthday attacks on	64-bit block ciphers (SWEET33	2)				Severe (5)	ssl-cve-2016-2183-sweet32	5 (AV:N/AC:L/Au	N/C:P/I:N/A:1	N) /	wg 24, 2016	Sep 2, 20	16
			DESCRIPTION legacy block ciphers having a should be the exhaustive seer with up to 2 to the power of n with 64-bit blocks, the birthda	block size of 64 bits are vulne ch of the key, with complexity 3 queries, but most modes of op y bound corresponds to only 33	rable to a practical collision a 2 to the power of k. However, eration (e.g. CBC, CTR, GCM, 2 GB, which is easily reached i	ttack when i he block siz OCB, etc.) a n practice. (used in CBC mo te n is also an in re unsafe with n Dnce a collision	de. All versions of the SSL/TLS protocols that support cipher suites oportant security parameter, defining the amount of data that can be nore than 2 to the power of half n blocks of message (the birthday be between two cipher blocks accurs it is possible to use the collision t	which use 3DES as the encrypted under the ound). With a modern to extract the plain te	he symmetric encryption cipher are affects same key. This is particularly important w block cipher with 128-bit blocks such as a xt data.	id. The security of i then using common AES, the birthday b	a block cipher n modes of op ound corresp	r is often ree peration: we onds to 256	duced to the ke require block (exabytes. How	y size k: the be ciphers to be so vever, for a bloo	st attack soure sk cipher
			NFFECTS													
			Asset 🗸	Name	Site	Port	Status	Proof					Last Sci	an	Exceptions	
			10.229.20.32	TAC-PC	TAC AAA	3389	Vulnerable Version	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA					Nov 24t	h, 2016	🖉 Exclude	

Risoluzione dei problemi

Debug su ISE

Per abilitare i debug su ISE, selezionare **Amministrazione > Sistema > Registrazione > Configurazione log di debug**, selezionare TC-NAC Node e modificare il componente **Log Level varuntime** e **va-service** in **DEBUG**.

dentity Servic	es Engine	Home	✓ ♦ Operations ♦ Policy	- Administration	► Work Centers
▼System Identity	Management •	Network Resources	rice Portal Management pxGrid	Services Feed Servic	e
Deployment Licens	ng Certificates	s ▼Logging ► Maintenar	nce Upgrade Backup & Resto	re Admin Access	▶ Settings
	0				
Local Log Settings		Node List > ISE21-3ek.exa Debug Level Configur	mple.com ration		
Remote Logging Targets		Debug Level conligu			
Logging Categories		/ Edit 🧐 Reset to Default	:		
Message Catalog		Component Name	▲ Log Level	Description	
Debug Log Configuration		va	8		
Collection Filters		○ va-runtime	DEBUG	Vulnerability Assessment	nt Runtime messages
		○ va-service	va-runtime DEBUG	Vulnerability Assessment	nt Service messages

Registri da controllare - varuntime.log. È possibile archiviarlo direttamente dalla CLI di ISE:

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

TC-NAC Docker ha ricevuto istruzioni per eseguire la ricerca di un endpoint specifico.

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 -::::- VA: received data from Mnt:

{"operationType":1, "macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","isPeriodicScanEn
abled":false,"heartBeatTime":0,"lastScanTime":0}

Una volta ricevuto il risultato, tutti i dati di Vulnerabilità vengono memorizzati nella directory di contesto.

```
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":"2.59999999","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"}]}
```

Registri da controllare - vaservice.log. É possibile archiviarlo direttamente dalla CLI di ISE:

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

```
L'adattatore ottiene i CVE insieme ai punteggi CVSS.
2016-11-24 12:45:33,132 DEBUG [SimpleAsyncTaskExecutor-2][]
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-key-
ciphers", "cveIds":"", "cvssBaseScore": "2.5999999", "vulnerabilityTitle": "TLS/SSL Server Supports
The Use of Static Key Ciphers", "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": "tls-dh-
prime-under-2048-bits", "cveIds":"", "cvssBaseScore":"2.5999999", "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},"time-
stamp":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
```

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

fe4e9fadadbd", "VendorName": "Rapid7 Nexpose", "OperationMessageText": "Number of endpoints queued for checking scan results: 0, Number of endpoints queued for scan: 0, Number of endpoints for

AdapterMessageListener controlla ogni 5 minuti lo stato dell'analisi fino al completamento.

NAC.AdapterInstanceUuid", "c2175761-0e2b-4753-b2d6-9a9526d85c0c", "TC-NAC.VendorName", "Rapid7 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"]}

adapter", "TC-NAC.Details", "VA request submitted to adapter for processing", "TC-NAC.MACAddress", "3C:97:0E:52:3F:D9", "TC-NAC.IpAddress", "10.229.20.32", "TC-

NAC.ServiceName", "Vulnerability Assessment Service", "TC-NAC.Status", "VA request submitted to

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

cpm.va.service.processor.AdapterMessageListener -::::- Message from adapter : {"AdapterInstanceName": "Rapid7", "AdapterInstanceUid": "7a2415e7-980d-4c0c-b5ed-

::::- VA SendSyslog systemMsg :

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

Richiesta di valutazione della vulnerabilità inviata alla scheda.

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

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-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"]}

Informazioni correlate

- Documentazione e supporto tecnico Cisco Systems
- Note sulla release di ISE 2.2
- Guida all'installazione dell'hardware ISE 2.2
- Guida all'aggiornamento a ISE 2.2
- Guida per l'amministratore di ISE 2.2 Engine