Konfigurieren von ISE 2.2 Threat-Centric NAC (TC-NAC) mit Rapid7

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Übergeordnetes Flussdiagramm Bereitstellen und Konfigurieren des Nexpose-Scanners Schritt 1: Bereitstellen des Nexpose-Scanners Schritt 2: Konfigurieren Sie den Nexpose-Scanner. **ISE konfigurieren** Schritt 1: Aktivieren Sie TC-NAC-Services. Schritt 2: Importieren des Zertifikats des Nexpose-Scanners. Schritt 3: Konfigurieren Sie die TC-NAC-Instanz des Nexpose Scanners. Schritt 4: Konfigurieren des Autorisierungsprofils zum Auslösen der VA-Prüfung Schritt 5: Konfigurieren von Autorisierungsrichtlinien Überprüfen **Identity Services Engine Nexus-Scanner** Fehlerbehebung Debugger auf der ISE Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie Threat-Centric NAC mit Rapid7 auf Identity Service Engine (ISE) 2.2 konfiguriert und behoben wird. Mit der Threat Centric Network Access Control (TC-NAC)-Funktion können Sie Autorisierungsrichtlinien erstellen, die auf den Bedrohungs- und Schwachstellenattributen basieren, die von den Adaptern für Bedrohungen und Schwachstellen empfangen wurden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Identity Service Engine
- Schwachstellen-Scanner

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Identity Service Engine Version 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

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

Konfigurieren

Übergeordnetes Flussdiagramm



Dies ist der Fluss:

- 1. Der Client stellt eine Verbindung zum Netzwerk her, der Zugriff ist beschränkt, und das Kontrollkästchen Schwachstellen bewerten ist aktiviert.
- 2. Der PSN-Knoten sendet eine Syslog-Meldung an den MNT-Knoten, in der bestätigt wird, dass die Authentifizierung erfolgt ist, und der VA-Scan war das Ergebnis der Autorisierungsrichtlinie.

- 3. Der MNT-Knoten sendet SCAN mithilfe der folgenden Daten an den TC-NAC-Knoten (unter Verwendung von Admin WebApp):
 - MAC-Adresse
 - IP-Adresse
 - Scan-Intervall
 - Periodischer Scan aktiviert
 - Ursprungs-PSN
- 4. Nexpose TC-NAC (in Docker-Container eingebettet) kommuniziert mit dem Nexpose Scanner, um bei Bedarf einen Scan auszulösen.
- 5. Nexpose Scanner scannt den von der ISE angeforderten Endpunkt.
- 6. Nexpose Scanner sendet die Ergebnisse der Prüfung an die ISE.
- 7. Die Ergebnisse der Prüfung werden an TC-NAC zurückgesendet:
 - MAC-Adresse
 - Alle CVSS-Bewertungen
 - Alle Sicherheitslücken (Titel, CVEIDs)
- 8. TC-NAC aktualisiert PAN mit allen Daten aus Schritt 7.
- 9. CoA wird bei Bedarf gemäß konfigurierter Autorisierungsrichtlinie ausgelöst.

Bereitstellen und Konfigurieren des Nexpose-Scanners

Vorsicht: Die Konfiguration in diesem Dokument für die Übungszwecke erfolgt nicht. Fragen Sie die Rapid7-Techniker, um Einzelheiten zum Design zu erfahren.

Schritt 1: Bereitstellen des Nexpose-Scanners

Der Nexpose-Scanner kann aus einer OVA-Datei bereitgestellt und auf Linux- und Windows-Betriebssystemen installiert werden. In diesem Dokument wird die Installation unter Windows Server 2012 R2 durchgeführt. Laden Sie das Image von der Rapid7-Website herunter und starten Sie die Installation. Wenn Sie **Typ und Ziel** konfigurieren, wählen Sie **Nexpose Security Console with local Scan Engine (Sicherheitskonsole mit lokalem Scan Engine) aus.**

	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	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
Installation success	Free disk space: 26,603 MB
RAPID	Cancel Previous Next

Nach Abschluss der Installation wird der Server neu gestartet. Nach dem Start sollte der Zugriff auf den Nexpose-Scanner über den 3780-Port erfolgen, wie im Bild gezeigt:



Wie im Bild gezeigt, durchläuft der Scanner den Systemstartprozess der Sicherheitskonsole:



Anschließend sollte der Lizenzschlüssel bereitgestellt werden, um Zugriff auf die GUI zu erhalten. Beachten Sie, dass die Enterprise Edition des Nexpose Scanners erforderlich ist. Wenn Community Edition installiert ist, werden Prüfungen nicht ausgelöst.

Schritt 2: Konfigurieren Sie den Nexpose-Scanner.

Der erste Schritt besteht in der Installation des Zertifikats auf dem Nexpose Scanner. Das Zertifikat in diesem Dokument wird von derselben Zertifizierungsstelle ausgestellt wie das Administratorzertifikat für die ISE (LAB CA). Navigieren Sie zu Administration > Global and Console Settings. Wählen Sie Administration unter Console aus, wie im Bild gezeigt.

=	nexpose [®] Create >				۵	54	@~	đ	۹	ු admin	
û											
88	2 lines	Asset Groupe	24 Evocations and Overrides		m o	landar					
¢	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	abilities from reports and to	View ca	lendar of all	scheduled sca	ns, blackouts	, database (operations	
	and password policy.	groups.	override policy compliance results.		and rep	orts.					
	Scan Options										
	ENGINES Create and manage available Scan El SHARED CREDENTIALS Create and manage shared credentia	ngines, and Scan Engine Pools. als for authenticated scans.	HISTORY	View current and past scans for this Create and manage scan templates	installation. for controlling	g and tuning	scans.				
	BLACKOUTS Create and manage global blackout s	settings.	ROOT CERTIFICATES	Manage root certificates used in sca	nning and wa	irehouse ex;	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 settings for the Security	risk score st Console, inch	rategies and uding auto-u	f excluding assigned	ets from scar	15.		
	CONNECTIONS Create and manage connections that	allow the Security Console to discover assets dynamically.		· ,							
	EVENTS View events and statistics for asset di	iscovery mechanisms.									

Klicken Sie auf Zertifikat verwalten, wie im Bild gezeigt:

≡	nexpose [®] Create V		
仚			
	Security Console Cont	figuration	
Ţ	GENERAL	The Security Console contains an embedde	ed web server. The following web server settings can be configured.
	UPDATES	WEB SERVER SETTINGS	
\oslash	WEB SERVER	Web server port	\$780
Q	PROXY SETTINGS	Session timeout (seconds)	600
	AUTHENTICATION	Maximum request handler threads	100
0	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

Klicken Sie, wie im Bild gezeigt, in **Neues Zertifikat erstellen**. Geben Sie **Common Name** und alle anderen Daten ein, die Sie im Identitätszertifikat des Nexpose Scanners speichern möchten. Stellen Sie sicher, dass die ISE in der Lage ist, Nexpose Scanner FQDN mit DNS aufzulösen.

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	

Exportieren der CSR-Anfrage (Certificate Signing Request) in das Terminal.



An diesem Punkt müssen Sie den CSR mit der Zertifizierungsstelle (Certificate Authority, CA) unterzeichnen.

The Security Co the CSR below	onsole has generated a c and send it to your CA fo	certificate signing re or signature. The signature of Certificate' butto	quest for the current ned certificate can la	certificate. You may ater be imported into	copy the
BEGIN NEW	CERTIFICATE REQUEST	-			1
MIJEYzCCAksC	AOAwHiEcMBoGA1UEAx	TbmV4cG9zZS5leG	tcGxlLmNvbTCCAilw		
DOYJKoZlhvcN	AOEBBOADaalPADCCAao	CaalBAIWOvirdSOIrD	wLMaHEISgHZoG4G		
ovg3oC9MeML	7s1TugD0K4pvmlZ0h1E+	B6bK7Z0B3QAnf9/V	Kaur/Q/yCNj1AcYH		
GB+Sq4bAfqHI	IKlsidnj3e00LW7h8TPm[057NOzOv4X8v6DOz	2YF8TNSmScbeTZ5		
q4qc9DH6RuY	JOEYawclWs+7wTVRDt+h	vFL6v6e6relXF7Nlp8	sqC02ZvDGzLnzb		
mwJFNG13BIL	ZykhiMzZVsnnGWAn9lghr	QRNftXW5JHYdFVs	4WeB+DKX1KWneigL		
rsay1voSprJXjr	cC3xAXHWQGFknY8d8ec	aEM82fUdzz6Y/jOqL	H6ToZ5mEAsKINg		
JEQpzLxjQsnA	ZRG8dy9+J52S6Zm7RXyC	g0p7MRKlykEOMGE	R5TF0ZWCfTxomvzp		
S0WExoXpWL8	oZbOtPHheWaQSmPStze	uQpiFXNjth/XQ0gHp	48v+1DdDeZI/wrLd		
j84GMbFuYvBc	+x08prU/kGEVftVABGHnj	nstGN+qM8CU93mq	6NNPmz8XCgAxCOm		
w/oD2cQFCdp	IXBC7cUdvkXMIJwqQXtp	d8uz9ZLvK+afJT8cBp	hledh1Fy+v7Mu+m		
OeNIx41XDaud	Lii/SuYBB03DLbN6Inu7Vp	+5/3W59lcfmHlt+3o	EJAnWx2vVCLgD		
NE /00E0W-00	FOLOTA-LADAAO-ADAAID	-I	OOA -FADNOLIOOKOT-		/

Importieren Sie das von der Zertifizierungsstelle ausgestellte Zertifikat, indem Sie auf Zertifikat importieren klicken.

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.

Konfigurieren einer Site Die Website enthält Ressourcen, die Sie scannen können sollten, und das Konto, das für die Integration der ISE mit dem Nexpose Scanner verwendet wird, sollte über Berechtigungen zum Verwalten von Standorten und zum Erstellen von Berichten verfügen. Navigieren Sie zu **Erstellen > Standort**, wie im Bild gezeigt.

CLOSE

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

Geben Sie, wie im Bild gezeigt, den **Namen** der Website auf der Registerkarte **Info & Security** ein. **Die** Registerkarte "**Assets**" sollte IP-Adressen der gültigen Ressourcen und Endpunkte enthalten,

die für die Schwachstellenüberprüfung qualifiziert sind.

=	nexpose Create 🗸						■ % 0~	ද <mark>ී</mark>
ô								
88	Site Configuration							SAVE & SCAN SAVE CANCEL
Ģ							<u>^</u>	
	INFO & SECURITY	ASSETS		TEMPLATES	¢ ENGINES		ALERTS	SCHEDULE
Ø								,
Q	GENERAL	General						
	ACCESS		Name AAA TAC		~			
0			Importance Normal		~			
=			Description					
		CUSTOM TAGS None	LOCAT	IONS	OWNERS None		CRITICALITY None	œ
								Add tags
=	nexpose [*] Create 🗸						≣ % ⊘~	ది
Û								
器	Site Configuration							SAVE & SCAN SAVE CANCEL
Q								
븃	INFO & SECURITY	C ASSETS		TEMPLATES	ENGINES			SCHEDULE
Ø								
â	Specify assets by Names/Addre	Sees Connection				_		
0	INCLUDE	No file selected			1 assets 🗸	EXCL	Accete Browne No fie selected	0 assets 🗸
0	Assets Browse W	to the selected.				0	Note brokse No the selected.	
⊨	10.229.20.32 × Enter nam	ne, address, or range.					Enter name, address, or range.	

Importieren Sie ein CA-Zertifikat, das das ISE-Zertifikat signiert hat, in den vertrauenswürdigen Speicher. Navigieren Sie zu Administration > Root Certificates > Manage > Import Certificates.

≡	nexpose	Create 🗸		‰ ⊙~	ି ଦ ବ	은 admin
						⊂ ITEMS ∨
Q	C	JSTOM CERTIFICATES 😡				^ ×
安		MPORT CERTIFICATES				
	C	stinguished Name	SHA-1 Fingerprint		Expires On	Delete
\odot	c	N-LAB CA, DC-example, DC-com	FD729A388533726FF84503	58A2F7EB27EC8A117	/8 02/12/2025	Î
Q						
ø	P	RESET CERTIFICATES				
0	C	stinguished Name	SHA-1 Fingerprint		Expires On	
ů.	c	N=DigiCert Assured ID Root CA, 0U=www.digicert.com, 0=DigiCert Inc, C=US	056388630D62D75A88C8A	31E48DF85A899824D	x43 11/10/2031	(
=	c	N+TC TrustCenter Glass 2 CA II, 0U-TC TrustCenter Glass 2 CA, 0-TC TrustCenter GmbH, C+DE	AE5083ED7CF45CBC8F61Cf	21FE685D794221156	SE 12/31/2025	j
	E	MAILADDRESS=premium-server@thavte.com, CN=Thavte Premium Server CA, OU=Certification Services Division, O=Thavte Consulting cc, L=Cape Town, ST=Western Cape, C=ZA	E0AB059420725493056062	023670F7CD2EFC666	.6 01/02/2021	1

ISE konfigurieren

Schritt 1: Aktivieren Sie TC-NAC-Services.

Aktivieren Sie TC-NAC Services auf einem ISE-Knoten. Beachten Sie:

- Für den Threat Centric NAC-Service ist eine Apex-Lizenz erforderlich.
- Sie benötigen einen separaten Policy Service Node (PSN) für den Threat Centric NAC-Service.

- Der Threat Centric NAC-Service kann auf nur einem Knoten in einer Bereitstellung aktiviert werden.
- Sie können pro Anbieter nur eine Instanz eines Adapters für den Vulnerability Assessment Service hinzufügen.

cisco Identi	ity Services I	Engine H	lome 🕨 C	Context Visibility	 Operations 	Policy	 Administration 	Work	Centers
▼System	Identity Ma	nagement 🕨 N	Network Reso	urces Device	Portal Manageme	ent pxGrid Se	rvices Feed Se	ervice 🕨	Threat Centric NAC
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade B	ackup & Restore	Admin Access	s 🕨 Setti	ings
Deploym	ent T		₩ .	Deployment Node Edit Node General Setting	s List > ISE22-1 e	ek a Configuration			
> တို့ Dr	ployment				Hostname ISE FQDN ISE IP Address 10. Node Type Ide	22-1ek 22-1ek.examp 48.23.86 entity Services	le.com Engine (ISE)		
				Personas					
				Administratio	'n		Role STAN	DALONE	Make Primary
				Monitoring			Role	MARY +	Other Monitoring Node
				Policy Service	2				
				🗹 Ena	ble Session Service	Personas ces	Include Nod	le in Node C	Group None v
				🗹 Ena	ble Profiling Servi	ice			
				Ena	ble Threat Centrie	c NAC Service			
				🗆 Ena	ble SXP Service	(i)	Use Interface	GigabitE	thernet 0 v
				🗆 Ena	ble Device Admin	Service			
				🗆 Ena	ble Passive Identi	ity Service			
				pxGrid (i					

Schritt 2: Importieren des Zertifikats des Nexpose-Scanners.

Importieren Sie das Zertifikat der Nexpose Scanner-Zertifizierungsstelle in den Trusted Certificates Store in der Cisco ISE (**Administration > Certificates > Certificate Management > Trusted Certificates > Import**). Stellen Sie sicher, dass die entsprechenden Root- und Zwischenzertifikate in den Cisco ISE Trusted Certificates Store importiert (oder vorhanden) werden.

dentity Services Engine	Home Context Visibility Operations Police	y ▼Administra	ation > Work Centers						Licens
System Identity Management	Network Resources Device Portal Management pxGr	id Services F	eed Service + Threat Cer	ntric NAC					Click here to do wireless setu
Deployment Licensing Certificate	es Logging Maintenance Upgrade Backup & Re	store + Admin	Access						chick here to do whereas setup
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	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	V
	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	2
	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	

Schritt 3: Konfigurieren Sie die TC-NAC-Instanz des Nexpose Scanners.

Hinzufügen von Rapid7-Instanzen unter Administration > Threat Centric NAC > Drittanbieter.

dentity Services Eng	ine Home	Context Visibility	Operations	Policy	▼ Adm	inistration	► W	ork Centers
System Identity Manage	ement • Network	Resources	e Portal Management	pxGrid S	ervices	Feed Sei	rvice	Threat Centric NAC ■
Third Party Vendors								
Vendor Instances > New Input fields marked with an asl	terisk (*) are required	d.						
Vendor *	Rapid7 Nexpose :	VA			•			
Instance Name *	Rapid7							
			C	ancel	ave			

Nach dem Hinzufügen wechselt die Instanz zum Status **Bereit zu Konfigurieren**. Klicken Sie auf diesen Link. Konfigurieren Sie **Nexpose Host** (Scanner) und **Port**, standardmäßig ist dies 3780. Geben Sie **Benutzername** und **Kennwort** mit Zugriff auf die richtige Site an.

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	
Password	
••••••	
Password of the user.	
Password of the user. Http proxy Host	
Password of the user. Http proxy Host Optional http proxy host. Requires proxy port also to be set.	
Password of the user. Http proxy Host Optional http proxy host. Requires proxy port also to be set. Http proxy port	
Password of the user. Http proxy Host Optional http proxy host. Requires proxy port also to be set. Http proxy port	
••••••• Password of the user. Http proxy Host Optional http proxy host. Requires proxy port also to be set. Http proxy port Optional http proxy port. Requires proxy host also to be set.	

Die erweiterten Einstellungen sind im ISE 2.2 Admin Guide gut dokumentiert. Sie finden den Link im Abschnitt Referenzen dieses Dokuments. Klicken Sie in **Weiter** und **Beenden**. Nexpose Instance wechselt in den **aktiven** Status, und der Download der Wissensdatenbank wird gestartet.

dentity Services Engine	Home Context	Visibility • Ope	erations Policy	 Administration 	Work Centers	
System Identity Management	Network Resources	Device Portal M	lanagement pxGrid S	ervices Feed Ser	vice Threat Centric NAC	
Third Party Vendors						
Vendor Instances						
C Refresh + Add i Tra	ash 🕶 🕑 Edit Rest	art Stop			▼ Filter ▼	¢
Instance Name	/endor Name	Туре	Hostname	Conne	ctivity Status	
Rapid7 F	Rapid7 Nexpose	VA	nexpose.example.com	Connec	ted Active	

Schritt 4: Konfigurieren des Autorisierungsprofils zum Auslösen der VA-Prüfung

Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile**. Neues Profil hinzufügen Aktivieren Sie unter **Häufige Aufgaben** das Kontrollkästchen **Schwachstellenbewertung**. Das On-Demand-Scan-Intervall sollte entsprechend Ihrem Netzwerkdesign ausgewählt werden.

Das Autorisierungsprofil enthält diese av-pair-Kräfte:

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 Sie werden innerhalb des Access-Accept-Pakets an Netzwerkgeräte gesendet, obwohl der eigentliche Zweck dieser Geräte darin besteht, dem Überwachungsknoten (MNT) mitzuteile

eigentliche Zweck dieser Geräte darin besteht, dem Uberwachungsknoten (MNT) mitzuteilen,
dass der Scan ausgelöst werden soll. MNT weist den TC-NAC-Knoten an, mit dem Nexpose
Scanner zu kommunizieren.
al al second

CISCO IDEITINY 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	Service Template
Profiling	Track Movement
► Posture	Passive Identity Tracking
Client Provisioning	
	Common Tasks Assess Vulnerabilities Adapter Instance Rapid7 • Trigger scan if the time since last scan is greater than 48 Enter value in hours (1-9999) • Advanced Attributes Settings ii Select an item • Attributes Details Access Type = ACCESS_ACCEPT cisco-arrivatire government-scan-intervalia:48
 Authorization Profiles Downloadable ACLs Profiling Posture Client Provisioning 	<pre>* Access Type ACCESS ACCEPT Network Device Profile Gisco Provide Translage Track Movement O Passive Identity Tracking O Passive Identity Tracking O * Common Tasks * Common Tasks * Common Tasks * Adapter Instance Repid7 Trigger scan if the time since last scan is greater than 48 Enter value in hours (1-9999) * Advanced Attributes Settings * Advanced Attributes Se</pre>

Schritt 5: Konfigurieren von Autorisierungsrichtlinien

• Konfigurieren Sie die Autorisierungsrichtlinie, um das in Schritt 4 konfigurierte neue

Autorisierungsprofil zu verwenden. Navigieren Sie zu **Richtlinien > Autorisierung > Autorisierungsrichtlinie**, suchen Sie die Regel **Basic_Authenticated_Access**, und klicken Sie auf **Bearbeiten**. Ändern Sie die Berechtigungen von **PermitAccess** in den neu erstellten **Standard Rapid7**. Dies führt zu einer Schwachstellenüberprüfung für alle Benutzer. Klicken Sie in **Speichern**.

isco Identi	ty Services Engine Home	Context Visibility Operations Policy Administration Wo	rk Centers	License Warning 🛆 🔍 🔍 🔘
Global Exce	ptions Policy Authentication Author	ization Profiling Posture Client Provisioning Policy Elements		Click here to do wireless setup and visibility setup Do not show this again
Authorizati Nefine the Aut for Policy Exp	horization Policy horization Policy by configuring rules base or go to Administration > System > Back	ed on identity groups and/or other conditions. Drag and drop rules to change the order μ & Restore > Policy Export Page	e.	
• Excentio	ans (1)			
Status	s Rule Name	Conditions (identity groups and other conditions)	Permissions	
	Exception Rule	If Threat:Rapid7 Nexpose-CVSS_Base_Score GREATER 1	then Quarantine	Edit I 🕶
Standard				
Status	s Rule Name	Conditions (identity groups and other conditions)	Permissions	
~	Wireless Black List Default	If Blacklist AND Wireless_Access	then Blackhole_Wireless_Access	Edt I •
	Profiled Cisco IP Phones	If Cisco-IP-Phone	then Cisco_IP_Phones	Edt I 🕶
	Profiled Non Cisco IP Phones	If Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones	Edt I 👻
0	Compliant_Devices_Access	If (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess	Edt (👻
0	Employee_EAP-TLS	If (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD	Edtiv
0	Employee_Onboarding	If (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD	Edt I 👻
	Wired_Guest_Access	If (Guest_Flow AND Wired_MAB)	then PermitAccess AND Guests	Edit I 👻
~	Wi-Fi_Guest_Access	If (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests	Edit I 👻
	Wired_Redirect_to_Guest_Login	if Wired_MAB	then Cisco_WebAuth	Edt I 👻
0	Wi-Fi_Redirect_to_Guest_Login	if Wireless_MAB	then Cisco_WebAuth	Edt I 👻
	Basic_Authenticated_Access	If Network_Access_Authentication_Passed	then Rapid7	Edt I 🔻
2	Default	if no matches, then DenyAccess		Edt I 🕶

Überprüfen

Identity Services Engine

Die erste Verbindung löst VA Scan aus. Wenn die Prüfung abgeschlossen ist, wird die CoA-Neuauthentifizierung ausgelöst, um neue Richtlinien anzuwenden, wenn sie abgeglichen werden.

cisco Ident	ity Services Engine	Home + Conte	ext Visibility	 Operations 	Policy Administration	n							License	Warning 🔺 🕓	
▼RADIUS	Threat-Centric NAC Live	Logs + TACACS	Troublesho	ot Adaptive	Network Control Reports							Click here to do	wireless setup	and visibility setup	Do not show this again. ×
Live Logs	Live Sessions														
		Misconfigured Su	pplicants O		Misconfigured Network De	evices O	RADIUS Drops	0	CI	ient Stopped Responding 0		Repeat Cou	nter O		
		0			0		0			0		0			
											Even: 1 minute	-law 1	test 20 mon	erte el u table	Last 24 hours
										Refresh	Every I minute	- Show La	1051 20 1000	- Within	Cash D4 Hours
C Refresh	Reset Repeat Count	ts 🔮 Export To 🕶								Refresh	Every Finincie	Show	1001 20 1000	within (▼ Filter • •
C Refresh Time	Reset Repeat Count	ts 💆 Export To 🗸	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authenticat	Authorizati	Authorization Profiles	IP Address	Network	k Device	Device Port	T Filter ▼ O ▼ Identity Group
C Refresh Time ×	Reset Repeat Count	ts A Export To - Status Status	Details	Repeat	Identity Identity	Endpoint ID Endpoint ID	Endpoint P Endpoint Prof	Authenticat	Authorizati	Authorization Profiles	IP Address IP Address	Network	k Device	Device Port Device Port	T Filter • • • • Identity Group
C Refresh Time ×	Reset Repeat Count 9 24, 2016 01:45:41.438 PM	ts 🛃 Export To - Status Status	Details	Repeat	Identity Identity alco	Endpoint ID Endpoint ID 3C:97:0E:52:3F:D9	Endpoint P Endpoint Profi Nortel-Device	Authenticat Authentication Default >> D	Authorizati Authorization Default >> E	Authorization Profiles Authorization Profiles Quarantine	IP Address IP Address 10.229.20.32	Network	k Device	Device Port Device Port FastEthernet 1/0/	▼ Filter ▼ ◆ ▼ Identity Group
C Refresh X Nov 2 Nov 2	 Reset Repeat Count 24, 2016 01:45:41.438 PM 24, 2016 01:45:40.711 PM 	ts Export To - Status Status	Details	Repeat	Identity Identity alco alco	Endpoint ID Endpoint ID 3C:97:0E:52:3F:D9 3C:97:0E:52:3F:D9	Endpoint P Endpoint Profi Nortel-Device Nortel-Device	Authenticat Authentication Default >> D Default >> D	Authorizati Authorization Default >> E Default >> E	Authorization Profiles Authorization Profiles Quarantine Quarantine	IP Address IP Address 10.229.20.32 10.229.20.32	Network	k Device	Device Port Device Port FastEthernet1/0/	Filter ← ↓ ← Identity Group Identity Group
Refresh Time X Nov 2 Nov 2 Nov 2	Reset Repeat Count 9 24, 2016 01:45:41.438 PM 24, 2016 01:45:41.438 PM 24, 2016 01:45:34.169 PM 24, 2016 01:45:39.166 PM	ts Export To - Status	Details 	Repeat 0	Identity Identity alice alice	Endpoint ID Endpoint ID 3C:97:9E:52:3F:09 3C:97:9E:52:3F:09 3C:97:9E:52:3F:09	Endpoint P Endpoint Profi Nortel-Device Nortel-Device	Authenticat Authentication Default >> D Default >> D	Authorizati Authorization Default >> E Default >> E	Authorization Profiles Authorization Profiles Quarantine Quarantine	IP Address IP Address 10.229.20.32 10.229.20.32	Network	k Device k Device	Device Port Device Port FastEthernet1/0/	T Filter • • • • Identity Group Identity Group 5 5 5 5

Um zu überprüfen, welche Schwachstellen erkannt wurden, navigieren Sie zu **Context Visibility > Endpoints**. Überprüfen Sie die Schwachstellen pro Endpunkt mit den vom Nexpose Scanner angegebenen Punktzahlen.

cisco	dentity S	ervices En	gine r	lome	▼ Context Visibilit	y Dpen	ations +	Policy	Administration	Work C	enters
Endpo	ints Us	ers Netwo	ork Devices								
Endpo	pints > 3	C:97:0E:52:3	F:D9								
					_						
3C	:97:0E	:52:3F:D	9 Ø	Ø	8						
	- 二	MAC Addre Username: Endpoint P Current IP Location: L	ess: 3C:97:08 alice Profile: Nortel- Address: 10.3 .ocation -> A	E:52:3F -Device 229.20.3 II Loca	:D9 32 tions						
	Applic	ations	Attributes	,	Authentication	Threats	Vulnerab	lities			
ssl-o	cve-2016-2	2183-sweet3	2								
Title	:	TLS/SSL Bi	irthday attack	s on 64	-bit block ciphers (SV	VEET32)					
CVS	S score:	5									
CVE	IDS:	CVE-2016-2	2183								
Rep	orted by:	Rapid7 Nex	rpose								
Rep	orted at:	Thu Nov 24	05:42:52 CE	T 2016							
ssi-	static-key-	ciphers	-								
Title		TLS/SSL S	erver Support	ts The L	Jse of Static Key Cip	hers					
CVS	S score:	2.5999999									
CVE	IDS:	_									
Rep	orted by:	Rapid7 Nex	pose								
Rep	orted at:	Thu Nov 24	05:42:52 CE	T 2016							
rc4-	cve-2013-	2566									
Title	:	TLS/SSL S	erver Support	s RC4	Cipher Algorithms (C	VE-2013-2566	3)				
CVS	S score:	4.30000019)								
CVE	IDS:	CVE-2013-2	2566								
Rep	orted by:	Rapid7 Nex	pose								
Rep	orted at:	Thu Nov 24	05:42:52 CE	T 2016							

Unter Operations > TC-NAC Live Logs (Vorgänge > TC-NAC Live-Protokolle) werden Autorisierungsrichtlinien und Einzelheiten zu CVSS_Base_Score angezeigt.

dentity Services Engine Home	Context Visibility Opera	tions Policy	Administration	• Work Centers				License Warning 🔺 🔍 🔍 🕯	o 6
RADIUS Threat-Centric NAC Live Logs Tr	ACACS > Troubleshoot > A	daptive Network Contro	Reports					Click here to do wireless setup and visibility setup Do not show this	again. ×
Threat Centric NAC Livelog									
C Refresh 💆 Export To 🕶 📕 Pause								T 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	

Nexus-Scanner

Wenn der VA-Scan durch die Übertragung des TC-NAC Nexpose Scan in den **In-Progress**-Zustand ausgelöst wird, und der Scanner beginnt, den Endpunkt zu überprüfen. Wenn Sie die Wireshark-Erfassung auf dem Endpunkt ausführen, wird an dieser Stelle der Paketaustausch zwischen der Endstation und dem Scanner angezeigt. Nach Abschluss des Scanners sind die Ergebnisse unter **Startseite** verfügbar.

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

Auf der Seite **Assets** (**Ressourcen**) können Sie sehen, dass neue Endgeräte mit den Ergebnissen des Scan verfügbar sind, das Betriebssystem identifiziert wird und 10 Schwachstellen erkannt werden.



Wenn Sie auf die **IP-Adresse** des **Endpunkts** klicken, wird der Nexpose-Scanner zum neuen Menü weitergeleitet, in dem Sie weitere Informationen wie Hostname, Risikobewertung und eine detaillierte Liste der Schwachstellen sehen können

=	nexp	ose	Create														đ		admin
û																			🛆 items 🗸
먦		TAC	AAA View all	sites															
Ģ																			
6			ADDRESSES	10.229.20.	32		OS	Kicrosoft Windows		RISK S	CORE 🔞				USER-ADDEC	TAGS 🔞			
30			HARDWARE	Unknown			CPE			ORI	SINAL		CUSTOM TA	GS		OW	INERS		
Ø			ALIASES	TAC-PC			LAST SCAN	Nov 24, 2016 4:42:07 AM (6 minutes ag	D)	2,	110		None			N	lone		
Q			HOST TYPE	Unknown			NEXT SCAP	Not set		CONTE	T-DRIVEN								Add tags
_			UNIQUE IDENTIFIERS							2,	016		LOCATION	S		CRIT	ICALITY		
2			SITE	TAC AAA															
Ø			SCAN ASSET NO	v C05	ATE ASSET DEDODT		T SENDLOG												
=			CONTRACT NO																
=	nexpo	ose	Create	~											в	<u></u>	Å	0	0
															74	0 *			📥 admin
		-												•	74	0.	~	~	i admin
Û		vı	ULNERABILITIE	s											γA	0.	Ŷ	~	<u>admin</u>
合 器		VL	ULNERABILITIE ew details about di	S	erabilities. To use one	of the exception co	ntrols on a vulnerabili	, select a row. To use the control with all displ	iyed displayed vulnerabil	lities, select the top row	and use Sele	ct Visible. Ca	ncel all selections using Clear All	0	ya		ų		<u>a</u> aomin
с в		Vie Die	ULNERABILITIE ew details about di posures: 發 Susc	S scovered vulni reptible to mal	erabilities. To use one Iware attacks 🔯 Me	of the exception co	ntrols on a vulnerabili	r, select a row. To use the control with all displ asploit J. Exploit published Jo	iyed displayed vulnerabil th published exploit	lities, select the top row	and use Sele	ct Visible. Ca	incel all selections using Clear All	0	¥4		Ę		<u>s</u> aomin
		VI Vie Eq	ULNERABILITIE ew details about di posures: 發 Susc EXCLUDE	S scovered vuln reptible to mal RECALL	erabilities. To use one Iware attacks @ Me RESUBMIT	of the exception co asploit-exploitable	ntrols on a vulnerabili	c select a row. To use the control with all display asploit (3), Exploit published 🍈 Validated wi	nyed displayed vulnerabil h published exploit	lities, select the top row	and use Sele	ct Visible. Ca	ncel all selections using Clear All	0	γ		Total Vuln	erabilities S	elected: 0 of 10
☆ 器 ◆			ULNERABILITIE ew details about di posures: & Susc EXCLUDE - Title	S scovered vuln reptible to main RECALL	erabilities. To use one Iware attacks W Me RESUBMIT	of the exception co	ntrols on a vulnerabili	r, select a row. To use the control with all displ asploin (2), Exploit published 🐧 Validated wi	nyed displayed vulnerabil	lities, select the top row	and use Seler	ct Visible. Ca CVSS	ncel all selections using Clear All Risk Publishe	0n	YA Modified On	Severity	Total Vuln	erabilities S Inces E	elected: 0 of 10 exceptions
			ULNERABILITIE ew details about di posures: & Susc EXCLUDE - Trite TLS/SSL Bi	S scovered vuln reptible to mail RECALL	erabilities. To use one ware attacks @ Me RESUBMIT	of the exception co aspfoit-exploitable rs (SWEET32)	ntrols on a vulnerabili	r, select a row. To use the control with all displ asploin (2), Exploit published 🐧 Validated wi	nyed displayed vulnerabil	lities, select the top row	and use Selec	ct Visible. Ca CVSS	ncel all selections using Clear All Risk Publishe 5 425 Wed Aug	d On 24 2016	VA Modified On Fri Sep 02 201	Severity v 6 Severe	Total Vuln	erabilities S ances E 1 (efected: 0 of 10 Xceptions
☆ ፡፡: � ⊘			ULNERABILITIE ew details about di posures: & Susc EXCLUDE - Title TLS/SSL Be TLS/SSL Be	S scovered vuln eptible to main RECALL thday attacks Supports TLS	erabilities. To use one Iware attacka @ Me RESUBMIT	of the exception co asploit exploitable rs (SWEET32)	ntrois on a vulnerabili	c select a row. To use the control with all displ	yyed displayed vulnerabil	lities, select the top now	and use Seler	ct Visible. Ca CVSS 4	Risk Publishe 5 425 Wed Aug 3 324 Tue Cet 1	d On 24 2016 4 2014	Modified On Fri Sep 02 201 Thu Nov 12 20	5 Severe 5 Severe	Total Vuln	erabilities S ances [1 (1 (elected: 0 of 10 ixceptions Disclude Disclude
℃ 器 ♥ ダ ♀			ULNERABILITIE ew details about di posures: & Sust EXCLUDE - Title - Title - TLS/SSL Be - TLS/SSL Se	S scovered vuln- eptible to main RECALL thday attacks Supports TLS river Supports	erabilities. To use one Iware attacka @ Me RESUBMIT s on 64-bit block ciphe version 1.0 IRC4 Cipher Algorithm	of the exception co asptoit-exploitable rs (SWEET32) a (CVE-2013-2566)	ntrois on a vulnerabili	r, select a row. To use the control with all displ aspioit	nyed displayed vulnerabilit	lities, select the top row	and use Selec	ct Visible. Ca CVSS 4.	Risk Publishe 5 425 Wed Aug 3 324 Tue Oct 1 3 397 Tue Mar	4 0n 24 2016 4 2014 12 2013	Modified On Fri Sep 02 201 Thu Nov 12 20 Thu Apr 28 20	Severity v 5 Severe 15 Severe 16 Severe	Total Vuin	erabilities S inces E 1 (1 (elected: 0 of 10 xxceptions 2 Exclude 2 Exclude 2 Exclude
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ </td <td></td> <td></td> <td>ULNERABILITIE ew details about di posures: & Susc EXCLUDE - Trale - Trale - TLS/SSL Be - TLS/SSL Se - TLS/SSL Se</td> <td>IS scovered vuln eptible to mal RECALL thday attacks Supports TLS river Supports river is enabling</td> <td>erabilities. To use on Iware attacks 🖗 Me RESUBMIT a on 64-bit block ciphe version 1.0 RC4 Cipher Algorithm g the BEAST attack</td> <td>of the exception co asploit-exploitable rs (SWEET32) a (CVE-2013-2566)</td> <td>ntrois on a vulnerabili</td> <td>r, select a row. To use the control with all displ sapioit 🔏 Exploit published 🏠 Valideted wi</td> <td>nyed displayed vulnerabilit</td> <td>lities, select the top row</td> <td>and use Selec</td> <td>ct Visible. Ca CVSS 4. 4. 4.</td> <td>Risk Publishe 5 425 Wird Aug 3 324 Tue Oct 3 397 Tue Mar 3 448 Tue Sep 1</td> <td>d On 24 2016 4 2014 12 2013 36 2011</td> <td>Modified On Fri Sep 02 201 Thu Nov 12 20 Thu Apr 28 20 Thu Feb 18 20</td> <td>Severity v 5 Severe 15 Severe 16 Severe</td> <td>Total Vuln</td> <td>erabilities S inces E 1 (1 (1 (1 (</td> <td>elected: 0 of 10 xxceptions 2 Exclude 2 Exclude 2 Exclude</td>			ULNERABILITIE ew details about di posures: & Susc EXCLUDE - Trale - Trale - TLS/SSL Be - TLS/SSL Se - TLS/SSL Se	IS scovered vuln eptible to mal RECALL thday attacks Supports TLS river Supports river is enabling	erabilities. To use on Iware attacks 🖗 Me RESUBMIT a on 64-bit block ciphe version 1.0 RC4 Cipher Algorithm g the BEAST attack	of the exception co asploit-exploitable rs (SWEET32) a (CVE-2013-2566)	ntrois on a vulnerabili	r, select a row. To use the control with all displ sapioit 🔏 Exploit published 🏠 Valideted wi	nyed displayed vulnerabilit	lities, select the top row	and use Selec	ct Visible. Ca CVSS 4. 4. 4.	Risk Publishe 5 425 Wird Aug 3 324 Tue Oct 3 397 Tue Mar 3 448 Tue Sep 1	d On 24 2016 4 2014 12 2013 36 2011	Modified On Fri Sep 02 201 Thu Nov 12 20 Thu Apr 28 20 Thu Feb 18 20	Severity v 5 Severe 15 Severe 16 Severe	Total Vuln	erabilities S inces E 1 (1 (1 (1 (elected: 0 of 10 xxceptions 2 Exclude 2 Exclude 2 Exclude
↑ 8 ♦ ♦ ∅ ∅ ∅ ∅ ∅ ∅ ∅ ∅ ∅ ∅ ∅			vv details about di vv details about di EXCLUDE Tale TLS/SSL Ba TLS/SSL Se TLS/SSL Se TLS/SSL Se	IS scovered vuln eptible to mal RECALL thdey attacks Supports TLS river Supports river is enablin river is enablin	erabilities. To use on hware attacks 🖗 Me RESUBMIT a on 64-bit block ciphe version 1.0 RC4 Cipher Algorithm g the BEAST attack Commonly Used Prim	of the exception co asploit exploitable to (SWEET32) to (CVE-2013-2566) to Numbers	ntrols on a vulnerabili	r, select a row. To use the control with all clapp asploit	yyed displayed vulnerabil h published exploit	lities, select the top now	and use Selec	ct Visible. Ca CVSS 4 4 4 2	Risk Publishe 5 425 Wed Aug 3 324 Tue Oct 3 440 Tue Sep 6 91.0 Wed Mag	4 On 24 2016 4 2014 12 2013 36 2011 20 2015	Modified On Fri Sep 02 201 Thu Nov 12 20 Thu Apr 28 20 Thu Feb 18 20 Thu Jen 16 20	Severity - 6 Severe 15 Severe 16 Severe 16 Severe 16 Severe	Total Vuin	ecobilities S inces E 1 (1 (1 (1 (1 (elected: 0 of 10 xxxeptions 2 Exclude 2 Exclude 2 Exclude 2 Exclude 2 Exclude
↑ ::::::::::::::::::::::::::::::::::::			UUNERABILITIE ev details about di pourses:	S scovered vuln eptible to mal RECALL thday attacks Supports TLS river Supports river is enablin river is using (an group sma	erabilities. To use one levere attacks I I Me RESUBMIT as on 64-bit block ciphe version 1.0 RC4 Cipher Algorithm rig the BEAST attack Commonly Used Prim lifer than 2048 bits	of the exception co asploit-exploitable is (OWEET32) is (OVEET32) is (OVEET32)	ntrols on a vulnerabili	r, select a row. To use the control with all displ asploit	yed displayed vulnerabil	lities, select the top now	and use Selec	CVSS 4 4 4 2 2	Risk Publishes A 425 Wed Aug 3 425 Wed Aug 3 448 Tue Get 4 48 Tue Sep 6 91.0 Wed May 6 91.0 Wed May	4 0n 24 2016 4 2014 12 2013 36 2011 20 2015 20 2015	Modified On Fri Sep 02 201 Thu Nov 12 20 Thu Apr 28 20 Thu Jan 16 20 Thu Jan 16 20 Thu Jan 16 20	Severity - 6 Severe 15 Severe 16 Severe 16 Severe 16 Severe 16 Moderate	Total Vuin Insta	erabilities S inces E 1 (1 (1 (1 (1 (1 (electrict 0 of 10 xceptions 2 Defuide 2 Defuide 2 Defuide 2 Defuide 2 Defuide 2 Defuide
↑ # ₩ Ø Q: Ø			UUNERABILITIE ev details about di pourses: 🔮 Susce CCCLUDE - Trate - Trate - TLS/SSL Se - TLS/SSL Se - TLS/SSL Se - TLS/SSL Se	S scovered vulne eptible to main RECALL thday attacks Supports TLS sover Supports river is enablin river is Using (an group sma inver Supports	erabilities. To use one RESUBMT on 64 bit block ciphe on 64 bit block ciphe BRGC Cipher Algorithm ig the BEAST ettack Commonly Used Prim lifer than 2048 bits The Use of Static Kip	of the exception co asplot-explorable (SWEET32) a (SWEET32) a (SWEET32) a (SWEET32) c) Pumbers	ntrols on a vulnerabili	r, select a row. To use the control with all displ asploit 👔 Exploit published 🔏 Validated wi	yed displayed vulnerabil	lities, select the top now	and use Selec	CVSS 4 4 2 2 2	Rak Publisher 5 425 Wed Aug 3 324 Tue Oct 1 3 3247 Tue Mar 3 448 Tue Sep 6 91.0 Wed Mag 6 240 Sun Feb	4 0n 24 2016 4 2014 12 2013 26 2011 20 2015 20 2015 20 2015	Modified On Fri Sep 02 201 Thu Nov 12 20 Thu Apr 28 20 Thu Feb 18 20 Thu Jun 16 20 Thu Jun 16 20 Wed Sep 30 21	Severity - 5 Severe 15 Severe 16 Severe 16 Severe 16 Moderate 15 Moderate	Total Vuln	erabilities S inces 5 1 1 1 1 1 1 1 1 1 1	ifected: 0 of 10 xxceptions 2 Exclude 2 Exclude 2 Exclude 2 Exclude 2 Exclude 2 Exclude 2 Exclude 2 Exclude 2 Exclude
℃ 器 〕 ☆ ⊘ & ⊡ @ Ⅲ			ULNERABILITII ever details about di porume:	S scovered vuln- eptible to mal RECALL thdey attacks Supports TLS river Supports river is unabilit river supports imp response	ersbilltes. To use on heure attacks 🖗 Me RESUBMIT a on 64-bit block cipher a on 64-bit block cipher a on 64-bit block cipher NRO Capher Algorithm RGC Capher Algorithm on the BEATS attack Community Lead Prim aller than 2048 bits The Use of Bastic Key	of the exception co asplot-explorable s (SWEET32) a (CVE-2013-2564) s Numbers Ciphers	ntrols on a vulnerability	r, select a row. To use the control with all displ	yyed displayed vulnerabil h published exploit	lities, select the top now	and use Selec	ct Visible. Ca CVSS 4. 4. 2. 2. 2.	Risk Publishe 5 425 Wed Aug 3 324 Tue Oct 3 347 Tue Mar 448 Tue Seg Tue Seg 6 91.0 Wed Mag 6 240 Sun Feb 6 240 Sun Feb 6 240 Sun Feb 0 0.0 Fit Aug	4 0n 24 2016 4 2014 12 2013 36 2011 20 2015 20 2015 20 2015 11 1997	Modified On Fri Sep 02 201 Thu Nov 12 20 Thu Apr 28 20 Thu Apr 28 20 Thu Jun 16 20 Thu Jun 16 20 Thu Nov 12 20 Wed Sep 30 21	Severity - 6 Severe 15 Severe 16 Severe 16 Severe 16 Moderate 15 Moderate 15 Moderate 2 Moderate	Total Vuin r insta	erabilities S ences E 1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (elected: 0 of 10 beceptions because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because because be
			ULNERABILITH ev details about di posures: 🔮 Sussi EXCLUDE - Tate - TuS/SSL 8 - TuS/SSL 9 - TuS/SSL 9 - TuS/SSL 9 - Diffe-Heller - Diff	S scovered vuln- eptible to mal RECALL thday attacks Supports TLS rver Supports rver is using (an group sma rver Supports amp response Traffic Amplit	erribilities. To use ono hware attacks 🖗 M& RESUBMIT I an 64-bit block cipher a on 64-bit block cipher version 1.0 RCG Capher Algorithm ing the BEAT attack Commonly Used Pitin ing the BEAT attack Commonly Used Pitin Sectors	of the exception co asploth exploitable is (DWEET32) is (CVE:2013-2566) Numbers Ciphers	nnnis en a vulnenbill Wildeted with Me	r, select a row. To use the control with all displ aspioit	yred displayed vulnerabil h published exploit	lities, select the top now	and use Selec	ct Visible. Ca CVSS 4. 4. 2. 2. 2.	Risk Publish 5 425 Wed Aug 3 324 Tue 0ct 3 347 Tue Mar 448 Tue Sep Wed Mag 91.0 Wed Mag Wed Mag 448 Tue Sep Wed Mag 5 0.0 Pin Aug 0 6 0.0 Pin Aug 0 0.0 Sun Feb	4 0n 24 2016 4 2014 12 2013 36 2011 20 2015 20 2015 20 2015 11 1997 29 2014	Modified On Fri Sep 02 201 Thu Nov 12 20 Thu Apr 28 20 Thu Apr 28 20 Thu Jun 16 20 Thu Jun 16 20 Thu Nov 12 20 Wed Sep 30 21 Thu Jul 12 20' Wed Sep 30 21	Severity - 6 Severe 15 Severe 16 Severe 16 Severe 16 Noderate 15 Moderate 15 Moderate 2 Moderate	Total Vuin	erabilities S inces I 1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (detects 0 of 10 biceptions biceptions biceptions biceute biceute biceute biceute biceute biceute biceute biceute biceute
			ULNERABILITH ev details about di pesures: United States TLS/SSL 56 TLS/SSL 56 TLS/SSL 56 TLS/SSL 56 TCP timests UP-P SSDP TLS/SSL 56	IS acovered vulne eptible to mal RECALL thdey attacks Supports TLS river Supports river is unablin river supports the supports river Supp	erabilities. To use once hware attacks i the second	of the exception co asptotr-exploitable rs (SWEET32) s (CVE-2013-2564) 1 Numbers Ciphers	ntrols on a vulnerabili	r, select a row. To use the control with all displ	yred displayed vulnerabil h published exploit	lities, select the top now	and use Selec	ct Visible. Ca CVSS 4. 4. 4. 2. 2. 2.	Risk Publishe 5 425 Wed Aug 3 324 Tue Oct 3 397 Tue Mar 4 Tue Sepi 91.0 Wed Mag 6 91.0 Wed Mag Wed Mag 6 91.0 Wed Mag Wed Mag 0 0.00 Sin Feb 91.0 0 0.00 Sin Feb 91.0	4 0n 24 2016 4 2014 12 2013 20 2015 20 2015 20 2015 11 1997 21 2015 21 2015	Modified On Fri Sep 02 201 Thu Nov 12 20 Thu Apr 28 20 Thu Jun 16 20 Thu Jun 16 20 Thu Jun 16 20 Thu Jul 12 20' Wed Sep 30 21 Thu Jul 12 20' Wed Dec 10 21 Mon Feb 15 21	Severity v 6 Severe 15 Severe 16 Severe 16 Moderate 115 Moderate 2 Moderate 114 Moderate	Total Vuin	erabilities 5 nnces I 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	vieteret 0 of 10 xceptions 2 Decivite 2 Decivite 2 Decivite 2 Decivite 2 Decivite 2 Decivite 2 Decivite 2 Decivite 2 Decivite

Wenn Sie auf die **Schwachstelle** selbst klicken, wird eine vollständige Beschreibung im Bild angezeigt.

	nexpo	se	Create										~ 4 [°]		ළ admir
															С ПЕМ
		v	ULNERABILITY INFOR	MATION											
		ov	VERVIEW												
		т	ītle						Severity	Vulnerability ID	CVSS		Published	Modified	
Q		т	LS/SSL Birthday attacks on	64-bit block ciphers (SWEET33	2)				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	,
		DE sh wit	ESCRIPTION gacy block ciphers having a ould be the exhaustive sear th up to 2 to the power of n th 64-bit blocks, the birthday	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	tack when u he block siz DCB, etc.) ar n practice. C	ised in CBC mo e n is also an in e unsafe with n Ince a collision	ds. All versions of the SSL/TLS protocols that support cipher suites portant security parameter, defining the amount of data that can be one than 2 to the power of half it blocks of massage (the bithday be between the cipher blocks accurs it is possible to use the collision t	which use 3DES as t encrypted under the ound). With a moderr to extract the plain te	e symmetric encryption cipher are affect same kay. This is particularly important v block cipher with 128-bit blocks such as et data.	ed. The security of when using commo AES, the birthday b	a block cipher is offu n modes of operatio sound corresponds to	en reduced to the k n: we require block o 256 exabytes. He	ey size k: the best c ciphers to be sec wever, for a block	Lattack sure c cipher
		AF	FECTS												
		^	aset 🗸	Name	Site	Port	Status	Proof				Las	it Scan	Exceptions	
		1	0.229.20.32	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				No	v 24th, 2016	Exclude	

Fehlerbehebung

Debugger auf der ISE

Um das Debuggen auf der ISE zu aktivieren, navigieren Sie zu Administration > System > Logging > Debug Log Configuration, wählen Sie TC-NAC Node aus, und ändern Sie die Protokollstufevaruntime und va-service-Komponente in 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 + Certificate	s -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 Carleset 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

Protokolle, die überprüft werden sollen - varuntime.log. Sie können sie direkt über die ISE-CLI entfernen:

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

TC-NAC Docker erhielt Anweisungen zur Durchführung der Prüfung auf einen bestimmten Endpunkt.

```
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","isPeriodicScanEn
abled":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-lek","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}

Sobald das Ergebnis empfangen wurde, werden alle Schwachstellendaten im Kontextverzeichnis gespeichert.

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\":\"sslstatic-keyciphers\",\"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-2048bits\",\"cveIds\":\"\",\"cvssBaseScore\":\"2.5999999\",\"vulnerabilityTitle\":\"Diffie-Hellman group smaller than 2048 bits\",\"vulnerabilityVendor\":\"Rapid7 Nexpose\"}","{\"vulnerabilityId\":\"tls-dhprimes\",\"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\",\"vulnerabilityId\":\"Rapid7 Nexpose\"}","{\"vulnerabilityId\":\"tlsv1_0enabled\",\"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-keyciphers", "cveIds":"", "cvssBaseScore": "2.5999999", "vulnerabilityTitle": "TLS/SSL Server Supports The Use of Static Key Ciphers", "vulnerabilityVendor": "Rapid7 Nexpose" }, { "vulnerabilityId": "rc4cve-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-dhprime-under-2048-bits", "cveIds":"", "cvssBaseScore":"2.5999999", "vulnerabilityTitle":"Diffie-Hellman group smaller than 2048 bits", "vulnerabilityVendor": "Rapid7 Nexpose"}, {"vulnerabilityId":"tls-dhprimes", "cveIds":"", "cvssBaseScore":"2.5999999", "vulnerabilityTitle":"TLS/SSL Server Is Using Commonly Used Prime Numbers", "vulnerabilityVendor": "Rapid7 Nexpose" }, { "vulnerabilityId": "sslcve-2011-3389-beast","cveIds":"CVE-2011-3389", "cvssBaseScore": "4.30000019", "vulnerabilityTitle": "TLS/SSL Server is enabling the BEAST attack", "vulnerabilityVendor": "Rapid7 Nexpose" }, { "vulnerabilityId": "tlsv1_0enabled", "cveIds":"", "cvssBaseScore":"4.30000019", "vulnerabilityTitle":"TLS Server Supports TLS version 1.0","vulnerabilityVendor":"Rapid7 Nexpose"}]}

Protokolle zu überprüfen - vaservice.log. Sie können sie direkt über die ISE-CLI entfernen:

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

Anfrage zur Schwachstellenbewertung wurde an Adapter gesendet.

2016-11-24 12:32:05,783 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 request submitted to 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.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"]}

AdapterMessageListener überprüft alle 5 Minuten den Status der Prüfung, bis sie abgeschlossen ist.

2016-11-24 12:36:28,143 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::- Message from adapter :
{"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
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":["TCNAC.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"]}]

Adapter erhält CVE's zusammen mit den CVSS Scores.

```
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":["TCNAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA successfully
completed","TC-NAC.Details","VA completed; number of vulnerabilities found: 7","TCNAC.MACAddress","3C:97:0E:52:3F:D9","TC-NAC.IpAddress","10.229.20.32","TCNAC.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"]}

Zugehörige Informationen

- <u>Technischer Support und Dokumentation Cisco Systems</u>
- ISE 2.2 Versionshinweise
- ISE 2.2 Hardware-Installationsanleitung
- ISE 2.2-Upgrade-Leitfaden
- ISE 2.2 Engine Administratoranleitung