

ConSol Software GmbH CM/Helpdesk - Vulnerability Management

Version 6.16

Inhalt

1	Vulnera	bility Management	3
	1.1 Ber	nutzeroberfläche Vulnerability Management	4
	1.1.1	Schwachstellen-Management Konfiguration	4
	1.1.2	Software-Ressourcen	5
	1.2 Vul	nerability Management einrichten	6
	1.2.1	Datenbank-Installationsskript ausführen	6
	1.2.2	Konfigurationsressource mit OpenCVE Zugangsdaten einrichten	6
	1.2.3	Ressource mit CVE-Datenbank verknüpfen	8
	1.3 Mit	dem Vulnerability-Management arbeiten	10
	1.3.1	CVE-Einträge abfragen	11
	1.3.2	CVE-Einträge entfernen	14
	1.3.3	Schwachstellen-Management-Tickets	15
2	Append	ix	18
	2.1 Ma	rken	18
	2.2 Glo	ssar	20

1 Vulnerability Management

Mit dem Vulnerability Management im CM/Helpdesk können Sie nach aktuellen **Sicherheitslücken** in den von Ihnen verwendeten Systemen scannen.

Wenn der Scan des Vulnerability Managements erkennt, dass ein neuer CVE (Common Vulnerabilities and Exposures) veröffentlich wurde, kann mit diesen Informationen im CM/Helpdesk automatisch ein Ticket eröffnet werden.

Für die Arbeit im Vulnerability Management gibt es im System zwei Rollen, sowie einen Bearbeiter:

- hd_vulnMgmtAdmin
- hd_vulnMgmtUser
- hd_vulnMgmtAgent

Wenn Sie sich als Benutzer mit den entsprechenden Berechtigungen im System anmelden, erhalten Sie auf dem Dashboard einen zusätzlichen Tab *Vulnerability Tickets*. Hier sehen Sie eine Übersicht aller Schwachstellen-Tickets im System.

bersicht									
Willkommen H	elpdesk Cockpit	Meine Aufgaben	Problems	Changes	Vulnerability Tickets	Reporting			
TICKETS MIT CVSS 3.0 EI	INSTUFUNG "KRITIS	FUNG "HOCH"	TICKETS MIT CVSS 3.0 EINS	TUFUNG "MITTI	EL"	TICKETS MIT CVSS 3.0 E	INSTUFUNG "NIEDRIG"		
4♥		_ 9	4	_	6♥			11 🖌 👘	
ALLE OFFENEN SCHWAC	HSTELLEN-	ALLE O	<u>FFENEN SCHWACHSTEI</u> <u>S</u>		ALLE OFFENEN SCHWACHS TICKETS	rellen-		ALLE OFFENEN SCHWAC TICKETS	
Schwachstellen-Tickets									
10 v Einträge anzeig	gen							Suchen	
Schwachstellen Ticket	Thema			Akt. Bearbeiter	Eröffnungsdatum	CVSS 2.0	CVSS 3.0	Hat Subtasks?	Letzte Änderung
101127	CVE-2020	-4027 in Atlassian Cont	fluence	Marc Respire	2022-11-16 12:44	6.5	4.7	Nein	2022-11-21 09:12

Abbildung 1: Vulnerability Management - Dashboard

1.1 Benutzeroberfläche Vulnerability Management

1.1.1 Schwachstellen-Management Konfiguration

Zum **Einrichten** der Schwachstellen-Management Konfiguration, wechseln Sie zum Abschnitt Konfigurationsressource mit OpenCVE Zugangsdaten einrichten.

Wenn Sie Ihre fertige Konfiguration auswählen, gewährt diese einen Überblick über die Detaildaten.

	Schwachstellen-Management Konfiguration & Konfigurationen Schwachstellen-Konfiguration	i	
	Intern Erstellt: 11.07.22 09:59 Benutzername der CVE-Schnittstelle Consol	Passwort der CVE-Schnittstelle	Verbindungsstatus
	URL zur API der Schnittstelle I /api	URL zur UI-Oberfläche der Schnittstelle /cve	Verbindung zu API-schnittstelle OK. Authentitizierung erfo
	Automatische Synchronisation aktiv? Soll-Wert: Aus Ist-Wert: Aus	Intervall-Einheit Täglich	Ausführungszeitpunkt der Synchronisation 00:00
	Zuletzt geändert um 16.11.2022 12:15		
È.	Detaildaten		
	Status der Synchronisation Abonnierte Objekte	Nicht abonnierte Objekte	
1	Status: Aktuell nicht am Synchronisieren		

Abbildung 2: Übersicht der Detaildaten einer Schwachstellen-Management Konfiguration

1. Konfigurationsdaten

Diese Daten werden beim Erstellen der Konfiguration angelegt.

- 2. Detaildaten
 - Status der Synchronisation

"Aktuell nicht am Synchronisieren" oder "Synchronisation in Arbeit"

Hier sehen Sie die wichtigsten Details zur aktuellen/letzten Synchronisation.

• Abonnierte Objekte

Hier sehen Sie alle **abonnierten** Software-Ressourcen (siehe Abschnitt <u>Ressource mit</u> <u>CVE-Datenbank verknüpfen</u>).

Status der Synchronisation	Abonnierte Objekte	Nicht abonnierte Objekte
Metabase Metabase		
Atlassian Confluence		
Debian Debian Linux		
Apache HTTP Server		

Abbildung 3: Abonnierte Objekte in einer Schwachstellen-Management Konfiguration

• Nicht abonnierte Objekte

Hier sehen Sie alle nicht abonnierten Software-Ressourcen.

1.1.2 Software-Ressourcen

Wenn Sie Ihre Software-Ressource ausgewählt haben, gewährt diese einen Überblick über die Detaildaten.

1. Basisdaten zur Software-Ressource

Diese Daten legen Sie beim Erstellen der Ressource an.

2. Detaildaten

Hier finden Sie die Detaildaten zu der erstellten Ressource.

Schwachstellen-Management Daten

Diese Daten sind relevant für die Synchronisation mit der Schnittstelle. Beachten Sie dazu den Abschnitt <u>Ressource mit CVE-Datenbank verknüpfen</u>.

• Bekannte Schwachstellen

Eine Liste der aktuell bekannten Schwachstellen in der CM Datenbank.

ſ	Ressou	rce metabase metabase @ IT Assets # Software			🖉 Bearbeiten	Als Favorit speichern	🚫 Deaktivieren	🗍 Lösche
		ntern Ersteirt 24.11.22, 12:18 Name metabase		Hersteller metabase				
		Detaildaten					🖄 Bi	earbeiten
		Schwachstellen-Management Daten Abonniert? Ja Hersteller metabase	Bekannte Schwachstellen	Schwachstellen Suchmodus Über Hersteller und Produkt Produkt metabase				
		Status: Aktuell nicht am Synchronis Status der vorherigen Synchroni Anzahl der neu hinzugefügten C Dauer der vorherigen Synchronis Zum Aktualisieren Seite erneut laden!	leren sation: Erfolgreich /E-Einträge: 11 sation: 00:00:01					

Abbildung 4: Übersicht einer Ressource-Software

1.2 Vulnerability Management einrichten

Beachten Sie, dass das Einrichten des Vulnerability Managements administrative Tätigkeiten in der *CM Web Admin Suite (WAS)* benötigt. Zögern Sie nicht, bei Fragen Ihren Consultant oder unseren Support zu kontaktieren. Gerne unterstützen wir Sie bei der Einrichtung oder schließen diese für Sie ab.

Voraussetzung: Ein OpenCVE-Account

Falls Sie noch keinen OpenCVE-API Account besitzen, erstellen Sie einen neuen Account (<u>https://www.opencve.io/welcome</u>). Beachten Sie zur Installation die offizielle Anleitung von OpenCVE (<u>https://docs.opencve.io/</u>).

1.2.1 Datenbank-Installationsskript ausführen

Damit die Schnittstelle ordnungsgemäß funktioniert, muss die Datenbank der ConSol CM-Installation ergänzt werden.

Dies erfolgt über ein Task-Skript.

- 1. Melden Sie sich in der Web Admin Suite als Administrator an.
- 2. Wählen Sie im Navigationsmenü auf der linken Seite Geschäftslogik > Skripte aus.
- 3. Suchen Sie in der Suchleiste nach dem Skript "hd_cve_db_install.groovy".
- 4. Klicken Sie das Skript an um es auszuwählen.
- 5. Klicken Sie auf Task ausführen, um das Skript auszuführen.

Die Datenbank ist jetzt bereit für die Verwendung der CVE-Schnittstelle.

1.2.2 Konfigurationsressource mit OpenCVE Zugangsdaten einrichten

Voraussetzungen:

- OpenCVE Installation und Account
- Datenbank-Installationsskript erfolgreich ausgeführt
- Benutzer mit der Rolle "hd_vulnMgmtAdmin", Standardlogin "hd_vulnMgmtAgent"
- 1. Melden Sie sich im Web Client mit dem entsprechenden Benutzer an.
- 2. Klicken Sie in der Navigationsleiste auf Ressourcenpool.

CM/ Helpdesk	Neues Ticket	Neuer Kontakt	Ressourcenpool	Online Hilfe
la la il du come En Al ancience		h Client		

3. Wählen Sie im Bereich *Konfigurationen > Schwachstellen-Konfiguration* die Auswahl "Neu erstellen".

	2					
•	Serviceverträge		IT Assets		Konfigurationen	
essourcen anzeige	n oder neu erstellen					
essourcen anzeiger	n oder neu erstellen	× If Amets		© Konfiguration	nen	
 serviceverträge 	n oder neu erstellen	× 11 Ameta		© Konfiguration	nen	_

Abbildung 6: Neue Schwachstellen-Konfiguration erstellen

- 4. Füllen Sie im Formular die Felder aus (Pflichtfelder sind markiert mit einem roten Stern *).
 - Benutzername und Passwort der CVE-Schnittstelle

Geben Sie hier Ihre Zugangsdaten zum API-Endpunkt ein.

• URL zur API und UI-Oberfläche der Schnittstelle

Geben Sie hier die URL zur API und UI der openCVE-Installation ein.

Wenn Sie die öffentliche OpenCVE-API verwenden, geben Sie bei der URL bitte folgendes an:

- API der Schnittstelle: <u>https://www.opencve.io/api</u>
- UI-Oberfläche der Schnittstelle: <u>https://www.opencve.io/cve</u>
- Setzen Sie die Checkbox für die Automatische Synchronisation auf "Aktiv".

Geben Sie eine Intervall-Einheit und den gewünschten Ausführungszeitpunkt der Synchronisation ein.

5. Klicken Sie auf *Ressource erstellen*.

Die Schwachstellen-Konfiguration in Ihrem ConSol CM-System ist jetzt angelegt.

Ressou	rce		🖉 Bearbeiten 😭 Als Favorit speichern 🚫 Deaktivieren 🗍 Löschen
	Schwachstellen-Management Konfiguration		
	Benutzername der CVE-Schnittstelle	Passwort der C/E-Schnittstelle	Verbindungsstatus
	URL zur API der Schnittstelle /api	URL zur UI-Oberfläche der Schnittstelle /cve	Verbindung zu API-Schnittstelle OK. Authentifizierung erfolgreich.
	Automatische Synchronisation aktiv? Soll-Wert: An Ist-Wert: Aus	Intervall-Einheit Täglich	Ausführungszeitpunkt der Synchronisation 02:00
	Zuletzt geändert um 24.11.2022 11:09		
	Detaildaten		🖉 Bearbeiten 🔺
	Status der Synchronisation Abonnierte Objekte Nicht abonnierte Objekte		
	Um Informationen über die aktuelle oder vorherige Synchronisation darsteller	n zu können, muss zuerst eine Synchronisation gestartet werden.	

Abbildung 7: Fertig angelegte Schwachstellen-Management Konfiguration im Web Client

1.2.3 Ressource mit CVE-Datenbank verknüpfen

Beachten Sie: Die öffentliche Schnittstelle (www.opencve.io/api) verfügt über ein Account-Limit. Hier sind jeweils nur 1000 CVE Abfragen pro Tag zulässig. Bedenken Sie dabei, dass auch schon einzelne Produkte mit einer großen Anzahl von CVEs dieses Tageslimit ausreizen können. Achten Sie deshalb darauf, nur die wichtigsten Software-Produkte zu abonnieren.

Möchten Sie mehr Einträge abrufen, empfehlen wir Ihnen, eine eigene Instanz der Lösung openCVE zu installieren.

Wenn Sie eine Ressource erstellt haben, verknüpfen Sie diese mit allen Endgeräten auf denen die Ressource installiert ist um einen bestmöglichen Schutz zu gewährleisten und Schwachstellen ausfindig zu machen.

1. Klicken Sie in der Navigationsleiste auf Ressourcenpool.



Abbildung 8: Navigationsleiste im Web Client

2. Wählen Sie im Bereich IT Assets > Software die Auswahl "Neu erstellen".

			0		
	Serviceverträge		IT Assets	Konfigurationen	
Ressourcen anzeigen	oder neu erstellen				~
- Serviceverträge		🗷 IT Assets		Konfigurationen	
Servicevertrag (SLA)		Endgerät	+ Neu ersteller	Schwachstellen-Konfiguration	+ Neu erstellen
		Software	+ Neversteller		



- 3. Füllen Sie die Felder im Formular aus.
 - Checkbox: Abonniert?

Hiermit legen Sie fest, ob diese Software später in der automatischen/manuellen Synchronisation mit der Schnittstelle synchronisiert werden soll.

Das Abonnieren verknüpft die Software-Ressource mit der Schwachstellen-Management Konfiguration.

• Schwachstellen Suchmodus

Hiermit legen Sie fest, welche Felder zur Synchronisation verwendet werden sollen.

"Über Hersteller und Produkt"

Durchsucht nach CVE-Einträgen zu exakt der eingetragenen OpenCVE-Software.

Die Felder Hersteller und Produkt müssen dafür befüllt sein.

Dies ist der bevorzugte Suchmodus

"Über Freitext-Suchfeld"

CVE-Einträge, die durch den Begriff im Feld *Suchbegriff* gefunden werden, werden ergänzt.

Es wird in der CVE-ID und in der Zusammenfassung alles CVE-Einträge gesucht.

Nützlich, wenn Sie sich für Software vorbereiten wollen, die noch nicht in OpenCVE hinterlegt ist.

• Hersteller, Produkt, Suchbegriff

Wird nur benötigt, wenn der Schwachstellen-Suchmodus entsprechend konfiguriert ist.

Schwachstellen-Management Daten	Bekannte	Schwachstellen			
		Schwachstellen Suchmodus			
Abonniert?		Über Hersteller und Produkt		·	
Hersteller		Produkt			
metabase	Х т	metabase	×	~	
Suchbegriff					

Abbildung 10: Beispielressource "metabase"

4. Klicken Sie auf *Ressource erstellen*.

1.3 Mit dem Vulnerability-Management arbeiten

Sie haben im Rahmen des Vulnerability-Managaments in Ihrem CM/Helpdesk-System verschiedene Handlungsmöglichkeiten.

• CVE-Einträge abfragen

Synchronisieren Sie Ihre angelegte Ressourcen-Software mit der OpenCVE Datenbank um Schwachstellen aufzudecken und zu behandeln.

• CVE-Einträge entfernen

Es ist möglich, dass Sie sich bei einer Synchronisation gegen eine Ticketerstellung entschieden haben, allerdings im Nachhinein feststellen, dass Sie zu einem CVE-Eintrag doch ein Ticket erstellen möchten. In diesem Fall können Sie den betroffenen CVE-Eintrag löschen und eine neue Synchronisation durchführen, bei der Sie die Ticketerstellung aktivieren.

Schwachstellen-Management-Tickets

Erstellen Sie Tickets in Ihrem CM/Helpdesk-System, um sofort Maßnahmen gegen erkannte Sicherheitslücken und Schwachstellen zu ergreifen.

1.3.1 CVE-Einträge abfragen

Sie haben unterschiedliche Möglichkeiten und Vorangehensweisen um in Ihrem CM/Helpdesk Vulnerability Management neue CVE-Einträge abzufragen.

- Automatische Synchronisation aller abonnierten Ressourcen-Software
- Manuelle Synchronisation der abonnierten Ressourcen-Software
- Manuelle Synchronisation von einzelner Ressourcen-Software

1.3.1.1 Automatische Synchronisation aktivieren

Voraussetzung: die Felder "Intervall-Einheit" und "Ausführungszeitpunkt der Synchronisation" müssen belegt sein (siehe Abschnitt Konfigurationsressource mit OpenCVE Zugangsdaten einrichten).



- 1. Klicken Sie auf Ressourcenpool in der Navigationsleiste.
- 2. Klicken Sie im Bereich Konfigurationen auf Schwachstellen-Konfiguration.

	Serviceverträge		IT Assets		Konfigurationen	
essourcen anzeige	n oder neu erstellen					
essourcen anzeiger • Serviceverträge	n oder neu erstellen	× If Assets		© Konfiguratione	n	
essourcen anzeiger - Serviceverträge Servicevertrag (SLA)	n oder neu erstellen	× IT Amets Endgesit	+ Neu er	© Konfiguratione	n Infiguration	+ Neu erstelle

Abbildung 11: Schwachstellen-Konfiguration auswählen

- 3. Wählen Sie mit einem Klick Ihre Konfiguration aus der Liste aus.
- 4. Wählen Sie die Workflow-Aktivität *Automatische Synchronisation starten* auf der rechten Seite.

Ressou	arce		🔄 Bearbeiten 🖞 Als Favorit speichern 🚫 Deaktivieren 📗 Löschen 📗	Aktivitäten	^
	Schwachstellen-Management Konfiguration			Synchronisiere alle abonnierten Objekte	
0.00	Konfigurationen + Schwachstellen-Konfiguration intern Erstellt: 13.07.22, 17:26			Automatische Synch Disation starten	
	Benufaenname der CVI Schultstelle Consol	Passeurt der CVI-Schoftstelle	Verbindung zu API-Schnittstelle OK. Authentifizierung erfolgreich.	Workspace	~
	URL zur API der Schnittstelle	URL zur UI-Oberfläche der Schröttstelle		Workspace ist leer Alle ungespeicherten	
	Automatische Spechronisation alth/ ¹ Soll-Wert: An Int-Wert: Aut	Intervall-Enhelt Täglich	Auführungsmitpanlit der Sprahverslatten 02.00	Anderungen werden automatisch hier abgeleg	(f.
	Zuletzt geleidert um			Favoriten	~
	24.11.2022 11:09			SAP kein Login	
				and the second s	

Abbildung 12: Workflow-Aktivitäten für die Schwachstellen-Management Konfiguration

Die automatische Synchronisation ist nun aktiv.

Klicken Sie die Workflow-Aktivität Automatische Synchronisation stoppen, um die automatische Synchronisierung zu deaktivieren.

1.3.1.2 Abonnierte Software synchronisieren

Sie können Ihre Schwachstellen-Management Konfiguration auch über die Suchfunktionen finden.

- 1. Klicken Sie auf Ressourcenpool in der Navigationsleiste.
- 2. Klicken Sie im Bereich Konfigurationen auf Schwachstellen-Konfiguration.

	1				
	Serviceverbilge		IT Austra	. Kortya	rationes
Ressourcen anzeigen o	oder neu erstellen				^
· Serviceverträge		× IT Assets		© Konfigurationen	
Serviceventrag (SLA)		Endgerät	+ Neu erstell	Schwachstellgn, Konfiguration	+ Neu erstellen
		Software	+ Neu erstell	len	

Abbildung 13: Schwachstellen-Konfiguration auswählen

- 3. Wählen Sie mit einem Klick Ihre Konfiguration aus der Liste aus.
- 4. Wählen Sie in den *Detaildaten* den Reiter "Abonnierte Objekte" aus um zu prüfen ob und wie viele Ressourcen abonniert sind.

Status der Synchronisation	Abonnierte Objekte	Nicht abonnierte Objekte	
Metabase Metabase			
Atlassian Confluence			
Debian Debian Linux			
Apache HTTP Server			

Abbildung 14: Abonnierte Ressourcen

Es muss mindestens eine Software in der Liste erscheinen, also im Vorfeld von Ihnen abonniert worden sein (siehe Abschnitt <u>Ressource mit CVE-Datenbank verknüpfen</u>), andernfalls ist die Synchronisation wirkungslos.

5. Wählen Sie die Workflow-Aktivität Synchronisiere alle abonnierten Objekte oben rechts aus.

Ressource		🖉 Bearbeiten 🖞 Als Favorit speichern 🚫 Deaktivieren 📳 Litschen	täten	^
Schwachstellen-Management Kenfiguration & Konfigurationen + Schwachstellen-Konfiguration		Synch abore	ronisiere alle liertet pbjekte	
intern Erstellt: 13.07.22, 17:26		Synch	ronisation starten	
Benufzername der Ci/E-Schriftstelle	Fannenet der CVE-Schröftstarlie	Verbindungsstatus		_
Consol	******	Verbindung zu API-Schnittstelle OK. Authentifizierung erfolgreich.	pace -	×.
URL zur API der Schwittstelle	URL zur UR-Oberfläche der Schriftstelle Jose	Work Alter	pace ist leer ngespeicherten	
Automatische Spechrunisation aktiv? Soli Wert An Int Wert Ant	internali Cinheit Taglich	Audilinungsanitpunkt der Synchranisation autor 82:00	ungen werden uttsch hier abgelegt.	
Zuletzt geländert um		Farming	ten -	4
24.11.2022 11:09		2 M	P kein Login	
		10 II	nton HE From 1	

Abbildung 15: Workflow-Aktivitäten für die Schwachstellen-Management Konfiguration

- 6. Wählen Sie im Formular aus, ob ein Ticket für neu gefundene CVE-Einträge eröffnet werden soll.
- 7. Klicken Sie Speichern und Weiter.

Die Synchronisation beginnt. Sie können den aktuellen Fortschritt in den *Detaildaten* im Tab "Status der Synchronisation" einsehen.

1.3.1.3 Einzelne Software synchronisieren

Sie können Ihre einzelne Software auch über die Suchfunktionen finden.

- 1. Klicken Sie auf Ressourcenpool in der Navigationsleiste.
- 2. Klicken Sie im Bereich IT-Assets auf Software.

28						
•	Serviceverträge		E IT Assets		1 Konfigurationen	-
essourcen anzeig	en oder neu erstellen					
rssourcen anzeig	en oder neu erstellen	🛪 IT Assets		* Koeligastionen		
essourcen anzeig • Serviceverträge Servicevertrag (SLA)	en oder neu erstellen	× IT Assets Endgerät	+ Neu ers	tellen	Agustion	+ Neu erstel

Abbildung 16: Ressourcen-Software auswählen

- 3. Wählen Sie mit einem Klick die gewünschte Ressource aus der Liste aus.
- 4. Wählen Sie die Workflow-Aktivität *Software mit Schwachstellen-Datenbank abgleichen* auf der rechten Seite.

Beachten Sie, beim Anlegen, Abschnitt <u>Ress</u>	dass dafür die Felo 'Bearbeiten der So ource mit CVE-Da	ldaten im Tab <i>Schwachstellen-Man</i> ıftware ausgefüllt werden müssen (<u>tenbank verknüpfen</u>).	agement Daten siehe auch
essource Allevalas Carllonae di IT Austin 1 Software Intern totalit 13.07.23, 17.28 Name	really	therefore the frace of genetices The frace of genetices The frace of the frace	atalien-
Detaildaten Detaildaten Schwachsbefen Management Dates Manmaer0 Ja	adhatain Shaahdalar Jahaala Dar Henalalar Sahaala	Endedite Compared the dig	ing.
technice aflassian Mater: Aituell recht am Synchronistieren = Mater: Aituell recht am Synchronistieren = Anatal der neu biorenflaten: Childran 1	Produkt confluence etch	Faultes Sub training Lippe of Cong 1 Workson Congress Workson Congress	*

Abbildung 17: Workflow-Aktivitäten für Ressourcen-Software

5. Wählen Sie im Formular aus, ob Sie Tickets für die neu gefundenen CVE-Einträge erstellen wollen.

Wenn Sie die Software zum ersten Mal synchronisieren, ist es ratsam "Nein" auszuwählen, da potentiell sehr viele ältere Einträge gefunden werden.

6. Klicken Sie auf Speichern und weiter.

Die Synchronisation beginnt. Sie können den aktuellen Status in den *Detaildaten* im Tab "Schwachstellen-Management Daten" einsehen.

1.3.2 CVE-Einträge entfernen

1.3.2.1 Einzelne CVE-Einträge löschen

Sie können Ihre Ressourcen-Software auch über die Suchfunktionen finden.

- 1. Klicken Sie auf Ressourcenpool in der Navigationsleiste.
- 2. Klicken Sie im Bereich IT-Assets auf Software.



Abbildung 18: Ressourcen-Software auswählen

- 3. Wählen Sie mit einem Klick die gewünschte Ressource aus der Liste aus.
- 4. Wählen Sie die Workflow-Aktivität Schwachstelle aus Liste entfernen auf der rechten Seite.

lessou	irce			() [*] Bearbeiten	🔅 Als Favorit speichern	O Deaktivieren	E Löschen		Aktivitäten	~
	Atlassian Confluence								Software mit Schwach Datenbank abgleichen	stellen-
	G IT Assets + Software intern Erstellt: 13.07.22, 17:28								Alle Schwachstellen au entfernen	is Liste
	Confluence		Hersteller Atlassian						Schwachstelle aus Liste entfernen	e
	Detaildaten					0f	Restates A		Workspace	^
	Schwachstellen Managment Daten	Bekannte Schwachstellen							Workspace ist leer Alle ungespeicherten Anderungen werden	
	Abarriart? Ja		Schwachstellen Suchmodus Ober Hersteller und Produkt						automatisch hier abge	ingt.
	Hersteller		Produkt						Favoriten	~
	atlassian		confluence						SAP kein Login	
	Status: Aktuell nicht am Synchron	isieren In efferer Echslerwich					_		Laptop HP Envy Windows Endgeria	
	Anzahl der neu hinzugefügten (Dauer der vorherigen Synchron	CVE-Eintrige: 1 ination: 00:00:02						6	Windows Endgeria	
	2um Aktualisieren Seite erneut laden?								Drucker im 1. Stool	

Abbildung 19: Workflow-Aktivitäten für Ressourcen-Software

5. Geben Sie im Formular die CVE-ID des CVE-Eintrags ein, den Sie löschen möchten.

Sie können nicht mehrere CVE-IDs in das Formularfeld eingeben.

6. Klicken Sie auf Speichern und weiter.

Der CVE-Eintrag wurde aus der Liste gelöscht und wird bei der nächsten Synchronisation wieder hinzugefügt.

1.3.2.2 Alle CVE-Einträge einer Software löschen

Sie können Ihre Ressourcen-Software auch über die Suchfunktionen finden.

- 1. Klicken Sie auf *Ressourcenpool* in der Navigationsleiste.
- 2. Klicken Sie im Bereich IT-Assets auf Software.

	1		e .		1	
	serviceversage		17 Access		Komparationen	
ssourcen anzeiger	oder neu erstellen					
ssourcen anzeige	n oder neu erstellen	× IT Assets		* Kodipation		
ssourcen anzeiger Serviceverträge nviceverträg (SLA)	n oder neu erstellen	× IT Assets Endgerät	+ Neu 1	erstellen	a seligeration	+ Neu erste

Abbildung 20: Ressourcen-Software auswählen

- 3. Wählen Sie mit einem Klick die gewünschte Ressource aus der Liste aus.
- 4. Wählen Sie die Workflow-Aktivität *Alle Schwachstellen aus Liste entfernen* auf der rechten Seite.

Issource		🔄 Bearbeiten 🛛 😭 Als Favorit speichern	O Deaktivieren 🔄 Löschen	Aktivitäten ^
Atlassian Confluence				Software mit Schwachstellen- Datenbank abgleichen
G IT Assets + Software Intern Erstellt: 13.07.22, 17:28				Alle Schwachstellen aus Liste
Tame Confluence	Atlassian			Schwachstelle aus Liste entfernen
Detaildaten			🛛 Bearbeiten 🔺	Workspace A
Schwachstellen Managment Dates Bek	annte Schwachstellen			Workspace ist leer Alle ungespeicherten Anderungen werden
Alcoreiset?	Schwachstellen Suchmarker Über Hersteller und Produkt			automatisch hier abgelegt.
Name and American Street St	Provide All			Favoriten A
atlassian	confluence			SAP kein Login
Status: Aktuell nicht am Synchronisieren	a Edularith			Laptop HP Envy Windows Endgerit
 Anzahl der neu hinzugefligten CVE-EI Dauer der vorherigen Synchronisatio 	etrilge: 1 er 00:00:02			> El baramundi-win Windows Endgerät
Zum Aktualisieren Seite erneut laden/				Drucker im 1. Stock

Abbildung 21: Workflow-Aktivitäten für Ressourcen-Software

5. Klicken Sie auf Speichern und weiter.

Alle CVE-Einträge zu der Software wurden aus der Liste gelöscht und werden bei der nächsten Synchronisation wieder hinzugefügt.

1.3.3 Schwachstellen-Management-Tickets

Voraussetzung zur Arbeit mit Schwachstellen-Management-Tickets:Standardbenutzer "hd_ vulnMgmtAgent"

Ein Schwachstellen-Ticket gewährt Ihnen einen Überblick über die wichtigsten Daten zur Einschätzung des Risikos der Schwachstelle.

1. Basisdaten des Tickets

Ticketnummer, Queue, Bearbeitungsstatus, der aktuelle Bearbeiter sowie das Erstellungsdatum

2. Workflow-Aktivitäten

Hier finden Sie die Workflow-Aktivitäten mit denen Sie das Schwachstellen-Management-Ticket durch den Prozess leiten können.

3. Ticketdaten

Hier finden Sie beispielweise die ID des CVE-Eintrages, die betroffenen Produkte, eine Einschätzung über die schwere sowie eine Zusammenfassung der Sicherheitslücke.

4. Verknüpfte Ressourcen

Die Ressourcen-Software, die mit dem CVE-Eintrag verknüpft ist.

5. Detaildaten

Hier sehen Sie die ausführliche, von der Schnittstelle abgerufene Antwort im JSON-Format.

Ticket			🖉 Daten bearbeiten	🟠 Als Favorit speichern	Duplizieren	C Drucke	en 📗	Workflow-Aktivitäten
10	14127 . CVF-2018-069	7 in Metabase Metabase						Wichtigen Kommentar
	Schwachstellen Management	In Bearbeitung & admin (1)	21.07.22, 16:43					Ticket schließen
							-1	Sub-Tasks erstellen
ID		Erstellungsdatum		Betroffene Produkte				
CVE-2018-0697		15.11.18		🕀 🗀 metabase			- 1	Workspace ^
CVSS 2.0		CVSS 3.0						Workspace ist leer Alle ungespeicherten
weatum 4.3	-	Wedium 6.1/10						Änderungen werden automatisch bier abgelegt
Cross-site script	.ing vulnerability in Metabase v	ersion 0.29.3 and earlier allows ren	note attackers to inject arbit	rary web script or HTML vi	ia unspecified vecto	rs.	- 14	
							- 1	Favoriten ^
Detaildaten					🕅 Daten b	earbeiten	~	Favoriten sind leer
							-1	Firmen oder Suchen in dieses
Vulnerability-I	Aanagment Response							Fenster, um sie als Favoriten zu speichern.
Abrufdatum								
28.11.22								
JSON-Antwort								
created_at	2018-11-15T15:29:00Z							
 Cvss Cwes 								
id: CVE-201	8-0697							
summary: (Cross-site scripting vulnerability	y in Metabase version 0.29.3 and ea	rlier allows remote attacker	s to inject arbitrary web sc	ript or HTML via			
unspecified updated at	vectors. :: 2018-12-17T17:33:00Z							
vendors								
							- 1	
	ünften Tickets				+ H	inzufügen	~	
Keine verkn	upren nexees		0.0.0					
Keine verkn								
Keine verkn	monte					inzulugen	·	
Keine verkn	nments		101		+ H			
Keine verkn Keine Attac	hments		•••		+ H			
Keine verkn Keine Attac Verknüpfte	hments Ressourcen (1)				+ H		^	
Keine verkn Keine Attack Verknüpfte Detailgrad Niee	hments Ressourcen (1) 'rig – Zeige (Nurzugewiesen	te Relationen →) Anzeigen als List			+ H		^	
Keine verkn Keine Attack Verknüpfte Detailgrad Niee X ff Assets	hments Ressourcen (1) Irig – Zeige (Nur zugewiesen	ee Relationen + Anzeigen als List	8 -		+ H		^	
Keine verkn Keine Attack Verknüpfte Detailgrad Niec XIT Assets betroffene Sof	hments Ressourcen (1) Hig - Zeige (Nur zugewiesen ware (1) + Hinz	e Relationen - Anzeigen als (List	•••		+ H		^	

Abbildung 22: Ansicht eines Schwachstellen-Management-Tickets

1.3.3.1 Schwachstellen-Tickets bearbeiten

1. Nehmen Sie das Ticket über die Workflow-Aktivität Annehmen an, um es weiter zu bearbeiten.

Bewerten Sie anhand der Ticketdaten, ob Ihre Systeme von der Schwachstelle betroffen sind. Lehnen Sie das Ticket ab, wenn das nicht der Fall ist.

- 2. Sie erhalten nun bei den Workflow-Aktivitäten neue Möglichkeiten zur Bearbeitung.
 - Wichtigen Kommentar hinzufügen

Über diese Aktivität können Sie einen Kommentar an das Ticket anhängen.

Dieser Kommentar wird automatisch auch an Subvorgänge angehängt.

• Ticket schließen

Sie können das Ticket abschließen und haben dabei außerdem die Möglichkeit, alle Subvorgänge mit abzuschließen.

• Sub-Tasks erstellen

Erstellen Sie beispielsweise ein Sub-Task pro betroffenem Endgerät, um den zugewiesenen Bearbeiter zu informieren, dass hier Handlungsbedarf besteht.

2 Appendix

Dieser Abschnitt enthält mehrere Appendizes:

• Marken

2.1 Marken

- Apache OpenOfficeTM Apache und die Apache-Federlogos sind Marken von The Apache Software Foundation. <u>OpenOffice.org</u> und das Mövenlogo sind eingetragene Marken von The Apache Software Foundation. Siehe <u>Website von Apache OpenOffice zu Markenrichtlinien</u>.
- Google MapsTM Google Maps ist eine Marke von Google Inc. Siehe <u>Google-Website über</u> <u>Marken</u>.
- HAProxy HAProxy ist Copyright von Willy Tarreau. Siehe HAProxy-Website.
- Microsoft[®] Microsoft und Windows sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Siehe <u>Website von Micro-</u><u>soft zu Markenrichtlinien</u>.
- Microsoft[®] Active Directory[®] Microsoft und Microsoft Active Directory sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Siehe <u>Website von Microsoft zu Markenrichtlinien</u>.
- Microsoft[®] Exchange Server Microsoft und Microsoft Exchange Server sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Siehe <u>Website von Microsoft zu Markenrichtlinien</u>.
- Microsoft[®] Office Microsoft und Microsoft Office sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Siehe <u>Website von Microsoft zu Markenrichtlinien</u>.
- Microsoft[®] Windows[®] Betriebssystem Microsoft und Windows sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Siehe Website von Microsoft zu Markenrichtlinien.
- Microsoft[®] SQL Server[®] Microsoft und Microsoft SQL Server sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Siehe <u>Website von Microsoft zu Markenrichtlinien</u>.
- Microsoft[®] Word[®] Microsoft und Microsoft Word sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Siehe <u>Website von Microsoft zu Markenrichtlinien</u>.
- MongoDB[®] Mongo, MongoDB und das MongoDB-Blattlogo sind eingetragene Marken von MongoDB, Inc.
- NGiNX NGiNX ist Copyright von Igor Sysoev und Nginx, Inc. Siehe <u>NGiNX-Lizenzseite</u>.
- OpenStreetMap OpenStreetMap[®] sind frei verfügbare Daten (Open Data), die unter Open Data Commons Open Database License (ODbL) von der OpenStreetMap Foundation (OSMF) lizenziert wurden. Siehe <u>OpenStreetMap Copyright- und Lizenzseite</u>.
- Oracle[®] Oracle ist eine eingetragene Marke von Oracle Corporation und/oder ihren verbundenen Unternehmen. Siehe <u>Website von Oracle zu Markenrichtlinien</u>.

- Oracle[®] WebLogic Oracle ist eine eingetragene Marke von Oracle Corporation und/oder ihren verbundenen Unternehmen. Siehe Website von Oracle zu Markenrichtlinien.
- Pentaho[®] Pentaho und das Pentaho-Logo sind eingetragene Marken von Pentaho Inc. Siehe <u>Website von Pentaho zu Markenrichtlinien</u>.
- Vis.js Vis.js ist Copyright von Almende B.V. Siehe Vis.js-Lizenzseite.
- Wicket[™] Apache Wicket und Wicket, Apache, das Apache-Federlogo und das Apache Wicket-Projektlogo sind Marken von The Apache Software Foundation. Siehe zum Beispiel den <u>Hinweis unten auf der Wicket-Homepage</u>

2.2 Glossar

<u>A</u>

ACF

ACF ist die Abkürzung von Activity Control Form (auf Deutsch Aktivitätsformular). ACFs können in Workflow-Aktivitäten verwendet werden, um den Bearbeiter zu zwingen, bestimmte Datenfelder auszufüllen, bevor er fortfahren kann.

Aktivität

Aktivitäten, auch Aktionen genannt, sind Vorgänge, die für Vorgänge, Kunden, Ressourcen und Suchergebnisse ausgeführt werden können.

В

Bearbeiter

Bearbeiter sind die Benutzer, die im Web Client an Vorgängen arbeiten.

Benutzerprofil

Das Benutzerprofil enthält die persönlichen Einstellungen, Vertretungen und Zeitbuchungen des Benutzers.

Berechtigung

Mit Berechtigungen wird festgelegt, welche Vorgänge der Bearbeiter im Web Client sehen kann und welche Aktionen er durchführen darf. Berechtigungen werden immer über Rollen erteilt, d.h. sie werden nicht einem einzelnen Benutzer zugewiesen, sondern einer Gruppe von Benutzern, die die gleiche Rolle haben. Normalerweise gehören diese Benutzer zum gleichen Team und/oder haben ähnliche Funktionen im Unternehmen.

Bereich

Der Workflow ist in unterschiedliche Bereiche aufgeteilt, die den Status eines Vorgangs zeigen.

Beteiligter

Beteiligte sind Benutzer, die einen bestimmten, im Geschäftsprozess definierten Zweck erfüllen. Normalerweise müssen sie im Prozess bestimmte Aufgaben ausführen.

С

CM/Doc

Ein ConSol CM-Standard-Modul, das es Bearbeitern ermöglicht, über den Web Client mit Microsoft Wordoder OpenOffice-Dokumenten zu arbeiten, die mit ConSol CM-Vorgangs- oder Kundendaten vorausgefüllt sind.

CM/Resource Pool

CM/Resource Pool ist ein optionales Add-on, das es ermöglicht, unterschiedliche Arten von Objekten als Ressourcen in ConSol CM zu speichern.

CM/Track

CM/Track ist das Portal von ConSol CM. Kunden erhalten über CM/Track Zugriff auf ihre Vorgänge.

D

Detailgrad

Der Detailgrad legt die in bestimmten Bereichen von Vorgängen, Kontakten und Ressourcen angezeigten Informationen fest.

F

Favoriten

Die Favoriten werden in einem Feld rechts neben dem Hauptarbeitsbereich angezeigt. Die Bearbeiter können Vorgänge, Kunden, Ressourcen und Suchen in die Favoriten ziehen und danach schnell öffnen.

Firma

Die Firma stellt die obere Hierarchiestufe in einem zweistufigen Kundenmodell dar. Eine Firma kann mehrere Kontakte haben.

G

Geschäftsprozess

Der Geschäftsprozess bestimmt, wie Vorgänge verarbeitet werden. Er bildet die Arbeit in Ihrem Team ab.

GUI

Graphical User Interface

Н

Hauptarbeitsbereich

Im Hauptarbeitsbereich wird das Element angezeigt, an dem der Bearbeiter gerade arbeitet. Dies kann ein Vorgang eine Kundenseite, eine Suchergebnisseite, ein Dashboard oder eine Ressourcenseite sein.

Hauptkunde

Der Hauptkunde ist der Kunde, der der Grund für die Erstellung des Vorgangs ist. In einem Vorgang muss ein Hauptkunde angegeben sein.

Hauptmenü

Das Hauptmenü wird im oberen Abschnitt der Seite angezeigt. Es enthält Links zu den unterschiedlichen Seiten des Web Clients.

Κ

Kontakt

Der Kontakt stellt die untere Hierarchiestufe in einem zweistufigen Kundenmodell dar. Ein Kontakt kann nur zu einer Firma gehören.

Kunde

Der Kunde stellt die externe Seite eines Vorgangs dar. Er ist die Person oder das Objekt, das den Grund für die Erstellung eines Vorgangs bildet. Ein Kunde kann entweder eine Firma oder ein Kontakt sein.

Kundendatenmodell

Das Kundendatenmodell ist die Definition der Kunden. Es bestimmt die verfügbaren Datenfelder und möglichen Relationen.

Kundengruppe

Die Kundengruppe bestimmt, welches Kundendatenmodell für ihre Kunden verwendet wird und welche Aktionen verfügbar sind.

L

LDAP

LDAP ist die Abkürzung für Lightweight Directory Access Protocol. Das ist ein Protokoll, mit dem Anmeldeinformationen für mehrere Applikationen verwaltet werden.

0

Overlay

Overlays sind kleine Symbole, die zum Vorgangs-Icon hinzugefügt werden, nachdem bestimmte Ereignisse eingetreten sind.

Ρ

PCDS

Page Customization Definition Section - Definitionsbereich der Seitenanpassung.

Protokoll

Das Protokoll enthält alle Änderungen, die an dem Vorgang, Kunden oder der Ressource ausgeführt wurden.

Q

Queue

Die Queue enthält thematisch ähnliche Vorgänge, die gleich behandelt werden sollen und dem gleichen Geschäftsprozess (Workflow) folgen. Berechtigungen und andere Parameter werden immer auf der Basis von Queues definiert.

R

Relation

Relationen sind Verknüpfungen zwischen unterschiedlichen Datenobjekten in ConSol CM. Es gibt Relationen zwischen Objekten des gleichen Typs, z.B. zwischen Vorgängen, Kunden und Ressourcen, und Relationen zwischen Objekten unterschiedlicher Typen, z.B. zwischen einem Vorgang und einer Ressource oder einem Kunden und einer Ressource.

Ressource

Ressourcen sind Objekte, die in CM/Resource Pool verwaltet werden.

Ressourcentyp

Der Ressourcentyp ist die Definition der Ressourcen. Er bestimmt die verfügbaren Datenfelder und möglichen Relationen und Aktionen.

Rolle

Rollen werden den Bearbeitern zugewiesen. Sie bestimmen die Zugangsberechtigungen und Sichten der Bearbeiter.

S

Session

Die Session ist der Zeitraum zwischen Anmeldung und Abmeldung im Web Client.

Sicht

Sichten beschränken die in der Vorgangsliste im ConSol CM Web Client angezeigten Vorgänge auf die Vorgänge, die bestimmte Kriterien (Bereiche eines oder mehrerer Workflows) erfüllen. Sichten werden Rollen zugewiesen.

V

Vertretung

Über die Vertretungsfunktion können Bearbeiter bestimmt werden, die einen Bearbeiter zeitlich begrenzt vertreten. Der Vertreter erhält eine Kopie aller E-Mails, die vom CM-System an die E-Mail-Adresse des Bearbeiters, den er vertritt, gesendet werden. Zudem hat die Vorgangsliste eine Option, mit der Vorgänge des vertretenen Bearbeiters angezeigt werden.

Vorgang

Der Vorgang ist die Kundenanfrage, an der der Bearbeiter arbeitet. Er ist das Objekt, das den vom Workflow definierten Geschäftsprozess durchläuft.

Vorgangs-Icon

Das Vorgangs-Icon wird in der oberen linken Ecke eines Vorgangs und in der Vorgangsliste angezeigt. Es hat normalerweise eine Farbe, die einen Wert eines bestimmten Parameters darstellt, und ein Symbol, das den aktuellen Bereich wiedergibt. Das Vorgangs-Icon kann Overlays haben.

Vorgangsliste

Die Vorgangsliste befindet sich links neben dem Hauptarbeitsbereich. Sie zeigt bestimmte Vorgänge auf einen Blick.

Vorlage

Vorlagen enthalten vordefinierten und vorformatierten Text. Sie können für Kommentare, E-Mails und Dokumente verwendet werden.

W

Web Client

Der Web Client ist der Hauptzugang zum System für die Bearbeiter.

Workflow

Der Workflow ist die Umsetzung des in ConSol CM verwalteten Geschäftsprozesses. Er enthält eine Reihe von Schritten, die von den Bearbeitern durchgeführt werden.

Workflow-Aktivität

Workflow-Aktivitäten werden dazu verwendet, Vorgänge durch den Geschäftsprozess zu bewegen.

Workspace

Der Workspace wird in einem Feld rechts neben dem Hauptarbeitsbereich angezeigt. Er dient als temporärer Speicher für Vorgänge, Kunden und Ressourcen, die geändert wurden, aber deren Änderungen noch nicht gespeichert wurden.

Ζ

Zeitbuchung

Zeitbuchungen ermöglichen es den Bearbeitern, die Zeit festzuhalten, die sie an einem Vorgang oder Projekt gearbeitet haben.

Zusatzkunde

Zusatzkunden sind Kunden (Firmen oder Kontakte), die am Vorgang interessiert sind. Sie sind optional und haben normalerweise eine Rolle, die anzeigt, wieso sie hinzugefügt wurden.