DISA STIG On Rocky Linux 8 (Italian version)

A book from the Documentation Team

Version : 2025/07/08

Rocky Documentation Team

Copyright © 2023 The Rocky Enterprise Software Foundation

Table of contents

1. Licence	3
2. HOWTO: STIG Rocky Linux 8 Fast - Part 1	4
2.1 Terminologia di riferimento	4
2.2 Introduzione	4
2.2.1 Passo 1: Creare la Macchina Virtuale	4
2.2.2 Passo 2: Scarica l'ISO Rocky Linux 8 DVD	5
2.2.3 Passo 3: Avviare l'Installatore	7
2.2.4 Passo 4: PRIMO Selezionare il Partizionamento	7
2.2.5 Fase 5: Configurazione del software per l'ambiente: Installazione del server senza interfaccia grafica	13
2.2.6 Passo 6: Selezionare Il Profilo Di Sicurezza	14
2.2.7 Fase 7: fare clic su "Done" e continuare con la Configurazione Finale	17
2.2.8 Passo 8: Creare un account utente e impostarlo come amministratore	17
2.2.9 Passo 9: Fare clic su "Done", e poi su "Begin Installation"	19
2.2.10 Passo 10: Una volta completata l'installazione, fate clic su "Reboot System"	20
2.2.11 Passo 11: Accesso al sistema Rocky Linux 8 STIG	21
2.3 Informazioni Sull'Autore	22
3. Introduzione	23
3.1 Elenco dei Profili di Sicurezza	23
3.2 Verifica della conformità DISA STIG	25
3.3 Generazione di script Bash di Riparazione	27
3.4 Generazione dei Playbook Ansible di Riparazione	29
3.5 Informazioni sull'Autore	31
4. Introduzione	32
4.1 Avvio rapido del server Apache 2.4 V2R5	32
4.2 Panoramica dei Controlli Dettagliati	33
4.2.1 Livelli	34
4.2.2 Tipi	34
4.3 Apache 2.4 V2R5 - Dettagli del Server	34
4.4 Informazioni sull'autore	45

1. Licence

RockyLinux offers Linux courseware for trainers or people wishing to learn how to administer a Linux system on their own.

RockyLinux materials are published under Creative Commons-BY-SA. This means you are free to share and transform the material, while respecting the author's rights.

BY : **Attribution**. You must cite the name of the original author.

SA : Share Alike.

• Creative Commons-BY-SA licence : https://creativecommons.org/licenses/by-sa/ 4.0/

The documents and their sources are freely downloadable from:

- https://docs.rockylinux.org
- https://github.com/rocky-linux/documentation

Our media sources are hosted at github.com. You'll find the source code repository where the version of this document was created.

From these sources, you can generate your own personalized training material using mkdocs. You will find instructions for generating your document here.

How can I contribute to the documentation project?

You'll find all the information you need to join us on our git project home page.

We wish you all a pleasant reading and hope you enjoy the content.

2. HOWTO: STIG Rocky Linux 8 Fast - Part 1

2.1 Terminologia di riferimento

- DISA Agenzia per i Sistemi Informativi della Difesa
- RHEL8 Red Hat Enterprise Linux 8
- STIG Guida all'Implementazione della Tecnica Sicura
- SCAP Protocollo di Automazione Sicura dei Contenuti
- DoD Dipartimento della Difesa

2.2 Introduzione

In questa guida verrà illustrato come applicare la DISA STIG per RHEL8 per una nuova installazione di Rocky Linux. Come serie in più parti, tratteremo anche come testare la conformità STIG, adattare le impostazioni STIG e applicare altri contenuti STIG in questo ambiente.

Rocky Linux è un derivato bug per bug di RHEL e come tale il contenuto pubblicato per il DISA RHEL8 STIG è in parità per entrambi i sistemi operativi. Una notizia ancora migliore è che l'applicazione delle impostazioni STIG è integrata nel programma di installazione di Rocky Linux 8 anaconda, sotto la voce Profili di Sicurezza. Il tutto è gestito da uno strumento chiamato OpenSCAP, che consente sia di configurare il sistema in modo che sia conforme alla DISA STIG (velocemente!), sia di testare la conformità del sistema dopo l'installazione.

Lo farò su una macchina virtuale nel mio ambiente, ma tutto ciò che è riportato qui si applica esattamente allo stesso modo su una macchina reale.

2.2.1 Passo 1: Creare la Macchina Virtuale

- Memoria 2G
- Disco 30G
- 1 core



2.2.2 Passo 2: Scarica l'ISO Rocky Linux 8 DVD

Scarica Rocky Linux DVD. **Nota:** La ISO minimale non contiene il contenuto necessario per applicare la STIG per Rocky Linux 8; è necessario utilizzare il DVD o un'installazione di rete.

	Download th	Downloads ne official release of Rocky Linux from o trusted mirrors. Rocky Linux 8 (Current) Planned EOL: May 31 2029	ne of our	
	ARCHITECTURE	ISOS	PACKAGES	
	x86_64	Minimal DVD Boot Torrent Checksum	BaseOS	
	ARM64 (aarch64)	Minimal DVD Boot Torrent Checksum	BaseOS	
Alternative Images	Cloud Images	Archived Releases	entation	Image: Second system Report Bug

2.2.3 Passo 3: Avviare l'Installatore

				rocky8-disa-stig on QEMU	J/KVM	_ c	- x
File \	/irtual Machine	View Send Key					
	💡 🕨	II 🗉 🔻	ē				÷
					ROCKY LINUX 8 INSTA	ALLATION	
					🖽 us	Help!	
	\sim						
	Q		WELCOME TO	ROCKY LINUX 8.			
	$\mathbf{\Omega}$		What language we	ld you like to use during the insta	llation process?		
			what language woo	ata you tike to use during the insta			
			English	English 🗲	English (United States)		
			Afrikaans	Afrikaans	English (United Kingdom)		
			አማርኛ	Amharic	English (India)		
			العربية	Arabic	English (Australia)		
			অসমীয়া	Assamese	English (Canada)		
			Asturianu	Asturian	English (Ireland)		
			Беларуская	Belarusian	English (New Zealand)		
	\times		Български	Bulgarian	English (Nigeria)		
			বাংলা	Bangla	English (Hong Kong SAR China)		
			⁴ 5:945	Tibetan	English (Philippines)		
			Bosanski	Bosnian	English (Singapore)		
			Català	Catalan	English (South Africa)		
			Čeština	Czech	English (Zambia)		
			Cymraeg	Welsh	English (Zimbabwe)		
			Dansk	Danish	English (Botswana)		
				B			
					Quit	Continue	

2.2.4 Passo 4: PRIMO Selezionare il Partizionamento

Questo è probabilmente il passo più complicato dell'installazione, e un requisito per essere conforme al STIG. È necessario partizionare il filesystem del sistema operativo in un modo che probabilmente creerà nuovi problemi. In altre parole: Avrai bisogno di sapere esattamente quali sono i tuoi requisiti di archiviazione.

🜢 Pro-Tip

Linux consente di ridimensionare i filesystem, di cui parleremo in un altro articolo. Basti pensare che questo è uno dei problemi più gravi dell'applicazione di DISA STIG su bare iron, che spesso richiede re-installazioni complete per essere risolto, quindi è necessario sovrastimare le dimensioni necessarie.



• Seleziona "Custom e poi "Done"

INSTALLATION DESTINATION	ROCKY LINUX 8 INSTALLATION
Done	🖼 us Help!
Device Selection	
Select the device(s) your like to install to. They will be left untouched until you click on the main mer	nu's "Begin Installation" button.
Local Standard Disks	
30 GiB	
Oxlaf4	
vda / 30 GiB free	
	Disks left unselected here will not be touched.
Specialized & Network Disks	
Add a disk	
	Disks left unselected here will not be touched.
Storage Configuration 🧢	
O Automatic	
Full disk summary and boot loader 1 disk	selected; 30 GiB capacity; 30 GiB free Refresh

• Inizia ad Aggiungere Partizioni



Schema di partizionamento DISA STIG per un disco 30G. Il mio caso d'uso è un semplice server web:

- / (10G)
- /boot (500m)
- /var (10G)
- /var/log (4G)
- /var/log/audit (1G)
- /home (1G)
- /tmp (1G)
- /var/tmp (1G)
- Swap (2G)

b Pro-Tip

Configurate / per ultimo e assegnategli un numero molto alto; in questo modo tutto lo spazio libero del disco rimarrà su / e non dovrete fare alcun calcolo.

MANUAL PARTITIONING					JX 8 INSTALLATION
 New Rocky Linux 8 Installation DATA /home rt-home /var/log rt-var_log /var/log/audit rt-var_log. 	1024 MiB 4 GiB 1024 MiB	rl-var Mount Point: /var Desired Capacity: 10 GiB		Device(s): 0x1af4 (vda) Modify	
/var/tmp rl-var_tmp SYSTEM /tmp rl-tmp /var rl-var swap rl-swap	ADD A NEW MOU More customize after creating the Mount Point: Desired Capacity:	JNT POINT ation options are available ne mount point below.	_ Encrypt	Volume Group:	(4 MiB free) 👻
+ - C' AVAILABLE SPACE TOTAL SPACE 9.99 GiB 30 GiB 1 storage device selected			Note: The be applied	settings you make o until you click on the	Update Settings a this screen will not e main menu's 'Begin Installation' button. Reset All
🗴 Pro-Tip					

Riprendendo il consiglio precedente: SOVRASTIMARE i filesystem, anche se in seguito dovrete farli espandere di nuovo.

• Clicca su "Done" e "Accept Changes"

MANUAL PARTITIONING				ROCKY LI	NUX 8 INS	TALLATION
Done				🖽 us		Help!
- New Rocky Linux 8 Installation		rl-root				
DATA /home rl-home	1024 MiB	Mount Point:		Device(s): Oxlaf4 (vda)		
/var/log rl-var_log	4 GiB	Desired Capacity:		Modify		
/var/log/audit rl-var_log_audit	1024 MiB	9.51 GiB				
/var/tmp rl-var_tmp	1024 MiB	Device Type:		Volume Group:		
SYSTEM	- 1	LVM 👻	Encrypt	rl	(0 B fi	ree) 👻
/	9.51 GiB >	File System:		Modify		
/tmp rl-tmp	1024 MiB	xfs Reform	nat			
/var rl-var	10 GiB					
/boot vdal	500 MiB	Label:		Name:		
swap rl-swap	2 GiB			root		
					Update S	Settings
+ - C			Note: The be applied	settings you make d until you click on	on this scre the main me	en will not nu's 'Begin
AVAILABLE SPACE 1023 KiB 30 GiB					Installati	on button.
1 storage device selected						Reset All

New Rocky Li	nux 8 lı	nstallation		rl	-700	t		
/home rl-home			1024	MiB	ount /	Point:	Device(s): Oxlaf4 (vda)	
/var/log	CLIMMA			~:D			Madify	
/var/log/au	Your cu	stomizations will	:> result in the following ch:	anges taking	effec	t after you return to the main mer	u and begin installation	n
rl-var_log_audi	Order	Action	Type	Device		Mount point		
/var/tmp	1	destroy format	Unknown	0x1af4 (vda	a)			
rl-var_tmp	2	create format	partition table (MSDOS)	0x1af4 (vda	a)			(0 B fron) =
SYSTEM	3	create device	partition	vda1 on 0x	, 1af4			(O B free)
1	4	create format	xfs	vdal on 0x	1af4	/boot		
rl-root	5	create device	partition	vda2 on 0x	1af4			
/tmp	6	create format	, physical volume (LVM)	vda2 on 0x	1af4			
rt-tmp	7	create device	lvmvg	rl				
/var d-var	8	create device	lvmlv	rl-var_log				
/boot	9	create format	xfs	rl-var_log		/var/log		
vdal	10	create device	lvmlv	rl-var_log_;	audit			
swap	11	create format	xfs	rl-var_log_;	audit	/var/log/audit		
rl-swap	12	create device	lvmlv	rl-tmp				
				Can	icel &	Return to Custom Partitioning	Accept Changes	
		_						Update Settings
						Note: T	he settings you make o	
+ - C							lied until you click on th	
AILABLE SPACE	TOTAL SE	ACE						

2.2.5 Fase 5: Configurazione del software per l'ambiente: Installazione del server senza interfaccia grafica

Questo avrà importanza in **Fase 6**, quindi se si utilizza un'interfaccia utente o una configurazione di workstation il profilo di sicurezza sarà diverso.

	ROCKY LINUX 8 INSTALLATIO
Base Environment	Additional software for Selected Environment
 Server with GUI An integrated, easy-to-manage server with a graphical interface. Server An integrated, easy-to-manage server. Minimal Install Basic functionality. Workstation Workstation is a user-friendly desktop system for laptops and PCs. Custom Operating System Basic building block for a custom Rocky system. Virtualization Host Minimal virtualization host. 	 Hardware Monitoring Utilities A set of tools to monitor server hardware. Windows File Server

2.2.6 Passo 6: Selezionare II Profilo Di Sicurezza

Questo configurerà una serie di impostazioni di sicurezza sul sistema in base al criterio selezionato, sfruttando il framework SCAP. Modificherà i pacchetti selezionati nella **Fase 5**, aggiungendo o rimuovendo i componenti necessari. Se *è stata* selezionata un'installazione con interfaccia grafica in **Fase 5** e si utilizza STIG non-GUI in questa fase, l'interfaccia grafica verrà rimossa. Regolatevi di conseguenza!



Selezionare DISA STIG per Red Hat Enterprise Linux 8:

TY POLICY			ROCKY LINUX 8 IN	STA
			🖽 us	
Change content	Apply security policy:			
Choose profile belov	w:			
parameters. Accord use in U.S. National	ingly, this configuration profile is s Security Systems.	suitable for		
PCI-DSS v3.2.1 Co Ensures PCI-DSS v3	ontrol Baseline for Red Hat Ente	erprise Linux 8 Is are applied.		
DISA STIG for Rec This profile contain DISA STIG for Red	I Hat Enterprise Linux 8 s configuration checks that align to Hat Enterprise Linux 8 V1R5.	o the		
In addition to being configuration baseli Red Hat technologi	applicable to Red Hat Enterprise L ne as applicable to the operating s es that are based on Red Hat Ente	.inux 8, DISA recognizes this system tier of srprise Linux 8, such as:		
 Red Hat Enterpris Red Hat Enterpris Red Hat Enterpris Red Hat Storage Red Hat Storage 	e Linux Server e Linux Workstation and Desktop e Linux for HPC	0 image		
DISA STIG with G	UI for Red Hat Enterprise Linux 8	o maye B		
		Select profile		
Changes that were c	lone or need to be done:			
💡 No profile selec	ted			

Fare clic su "Select Profile" e prendere nota delle modifiche che verranno apportate al sistema. In questo modo si impostano le opzioni sui punti di montaggio, si aggiungono/rimuovono le applicazioni e si apportano altre modifiche alla configurazione:

Cha	anges that were done or need to be done:
	prenage user addont retriewops has been added to the ast of exemption prenages
8	package 'xorg-x11-server-Xorg' has been added to the list of excluded packages
8	package 'vsftpd' has been added to the list of excluded packages
8	package 'abrt-plugin-logger' has been added to the list of excluded packages
8	package 'abrt-cli' has been added to the list of excluded packages
8	package 'xorg-x11-server-utils' has been added to the list of excluded packages
R	package 'python3-abrt-addon' has been added to the list of excluded packages

Chang	ges that were done or need to be done:
O-P	ласкаде ропсусотенных нах оеен аннен со сле нэс от со ве позаней раскадех
8 p	backage 'usbguard' has been added to the list of to be installed packages
💡 p	backage 'tmux' has been added to the list of to be installed packages
💡 p	backage 'rsyslog-gnutls' has been added to the list of to be installed packages
8 p	package 'rsyslog' has been added to the list of to be installed packages
💡 p	backage 'firewalld' has been added to the list of to be installed packages
	hackage 'openssI-nkcs11' has been added to the list of to be installed nackages

2.2.7 Fase 7: fare clic su "Done" e continuare con la Configurazione Finale



2.2.8 Passo 8: Creare un account utente e impostarlo come amministratore

Nelle esercitazioni successive potremo unire il tutto a una configurazione aziendale FreeIPA. Per il momento, lo tratteremo come un documento a sé stante. Notate che non sto impostando una password di root, piuttosto diamo l'accesso al nostro utente predefinito sudo.

CREATE USER		ROCKY LINUX 8 INSTALLATION
Full name	sshinn	j
User name	sshinn	
	Make this user administrator	
Bassword	Require a password to use this account	
rassworu	Strong	
Confirm password	••••••	
	Advanced	

2.2.9 Passo 9: Fare clic su "Done", e poi su "Begin Installation"



2.2.10 Passo 10: Una volta completata l'installazione, fate clic su "Reboot System"

Rocky Linu	INSTALLATION PROGRESS	ROCKY LINUX 8 INSTALLATION
×	1	Quit Reboot System

2.2.11 Passo 11: Accesso al sistema Rocky Linux 8 STIG



Se tutto è andato bene, si dovrebbe vedere il banner di avviso predefinito del DoD.



2.3 Informazioni Sull'Autore

Scott Shinn è il CTO per Atomicorp e fa parte del team Rocky Linux Security. Dal 1995 si occupa di sistemi informativi federali presso la Casa Bianca, il Dipartimento della Difesa e l'Intelligence Community. Parte di questo è stata la creazione degli STIG e l'obbligo di usarli, e mi dispiace molto per questo.

3. Introduzione

Nell'ultimo articolo abbiamo configurato un nuovo sistema rocky linux 8 con lo stig DISA applicato utilizzando OpenSCAP. Ora ci occuperemo di come testare il sistema usando gli stessi strumenti e di quali tipi di rapporti possiamo generare usando gli strumenti oscap e la sua controparte UI SCAP Workbench.

Rocky Linux 8 (e 9!) include una suite di contenuti SCAP per verificare e correggere la conformità a vari standard. Se avete costruito un sistema STIG nella prima parte, lo avete già visto in azione. Il programma di installazione di anaconda ha sfruttato questo contenuto per modificare la configurazione di rocky 8 per implementare vari controlli, installare/rimuovere pacchetti e cambiare il modo in cui funzionano i punti di mount a livello di sistema operativo.

Nel corso del tempo, questi aspetti potrebbero cambiare e sarà opportuno tenerli sotto controllo. Spesso utilizzo questi rapporti anche per dimostrare che un determinato controllo è stato implementato correttamente. In ogni caso, Rocky ne è dotato. Inizieremo con alcune nozioni di base.

3.1 Elenco dei Profili di Sicurezza

Per elencare i profili di sicurezza disponibili, è necessario utilizzare il comando oscap info fornito dal pacchetto openscap-scanner. Questo dovrebbe essere già installato nel vostro sistema, se avete seguito la procedura dalla prima parte. Per ottenere i profili di sicurezza disponibili:

oscap info /usr/share/xml/scap/ssg/content/ssg-rl8-ds.xml

🖍 Nota

Il contenuto di Rocky linux 8 utilizzerà il tag "rl8" nel nome del file. In Rocky 9, sarà "rl9".

Se tutto va bene, si dovrebbe ricevere una schermata simile a questa:

+ sshinn@winona6:~/src/aw	vp-agent/src/awp-agent/active-response — ssh 192.168.122.174 Q = ×
Document type: Source Data Str	eam
Imported: 2022-04-29T22:32:36	
Stream: scap_org.open-scap_dat Generated: (null) Version: 1.3	astream_from_xccdf_ssg-rl8-xccdf-1.2.xml
Checklists:	con crof con rl0 yoodf 1 0 yml
Status: draft	scap_crer_ssg-rto-xccur-1.2.xmc
Generated: 202	2-04-30
Resolved: true Profiles:	
Title:	ANSSI-BP-028 (enhanced)
Title:	Id: xccdf_org.ssgproject.content_profile_anssi_bp28_enhanced ANSSI-BP-028 (high)
Title:	Id: xccdf_org.ssgproject.content_profile_anssi_bp28_high ANSSI-BP-028 (intermediary)
Title:	<pre>Id: xccdt_org.ssgproject.content_profile_anssi_pp28_intermediary ANSSI-BP-028 (minimal) Id: vccdf_org_ssgproject_content_profile_anssi_hp28_minimal</pre>
Title:	CIS Red Hat Enterprise Linux 8 Benchmark for Level 2 - Server
	Id: xccdf_org.ssgproject.content_profile_cis
Title:	CIS Red Hat Enterprise Linux 8 Benchmark for Level 1 - Server
Title:	CIS Red Hat Enterprise Linux 8 Benchmark for Level 1 - Workstation
Title:	CIS Red Hat Enterprise Linux 8 Benchmark for Level 2 - Workstation Id: xccdf org.ssgproject.content profile cis workstation 12
Title:	Unclassified Information in Non-federal Information Systems and Organiz
ations (NIST 800-171)	
	Id: xccdf_org.ssgproject.content_profile_cui
Title:	Australian Cyber Security Centre (ACSC) Essential Eight
Title:	Health Insurance Portability and Accountability Act (HIPAA)
111101	Id: xccdf org.ssgproject.content profile hipaa
Title:	Australian Cyber Security Centre (ACSC) ISM Official
	Id: xccdf_org.ssgproject.content_profile_ism_o
Title:	Protection Profile for General Purpose Operating Systems
Titler	IG: XCCGT_OFG.SSGPFOJECT.CONTENT_PFOTILE_OSPP
Titte:	$Td \cdot xccdf$ arg scaproject content profile pci-dss
Title:	DISA STIG for Red Hat Enterprise Linux 8
	Id: xccdf_org.ssgproject.content_profile_stig
Title:	DISA STIG with GUI for Red Hat Enterprise Linux 8
	Id: xccdf_org.ssgproject.content_profile_stig_gui
Referenced che	CK TILES:
ssg-ri	system: http://oval mitre.org/XMLSchema/oval-definitions-5
· · · · · · · · · · · · · · · · · · ·	
[5] 0:bash*	"rocky8-disa-stig" 15:02 11-Jun-22

DISA è solo uno dei tanti profili di sicurezza supportati dalle definizioni SCAP di Rocky Linux. Abbiamo anche profili per:

- ANSSI
- CIS
- Australian Cyber Security Center
- NIST-800-171
- HIPAA
- PCI-DSS

3.2 Verifica della conformità DISA STIG

Qui è possibile scegliere tra due tipi:

- stig Senza interfaccia grafica
- stig_gui Con una GUI

Eseguire una scansione e creare un rapporto HTML per il DISA STIG:

sudo oscap xccdf eval --report unit-test-disa-scan.html --profile stig /usr/ share/xml/scap/ssg/content/ssg-rl8-ds.xml

Il risultato sarà un rapporto come questo:

Ð	sshinn@winona6:~/src/awp-agent/src/awp-agent/active-response — ssh 192.168.122.174 Q = ×
Result	pass
Title Rule Result	<pre>Verify User Who Owns /var/log Directory xccdf_org.ssgproject.content_rule_file_owner_var_log pass</pre>
Title Rule Result	<pre>Verify User Who Owns /var/log/messages File xccdf_org.ssgproject.content_rule_file_owner_var_log_messages pass</pre>
Title	Verify Permissions on /var/log Directory
Rule	xccdf_org.ssgproject.content_rule_file_permissions_var_log
Result	pass
Title	Verify Permissions on /var/log/messages File
Rule	xccdf_org.ssgproject.content_rule_file_permissions_var_log_messages
Result	pass
Title	Verify that Shared Library Directories Have Root Group Ownership
Rule	xccdf_org.ssgproject.content_rule_dir_group_ownership_library_dirs
Result	pass
Title	Verify that Shared Library Directories Have Root Ownership
Rule	xccdf_org.ssgproject.content_rule_dir_ownership_library_dirs
Result	pass
Title	Verify that Shared Library Directories Have Restrictive Permissions
Rule	xccdf_org.ssgproject.content_rule_dir_permissions_library_dirs
Result	pass
Title	Verify that system commands files are group owned by root
Rule	xccdf_org.ssgproject.content_rule_file_groupownership_system_commands_dirs
Result	pass
Title	Verify that System Executables Have Root Ownership
Rule	xccdf_org.ssgproject.content_rule_file_ownership_binary_dirs
Result	pass
Title	Verify that Shared Library Files Have Root Ownership
Rule	xccdf_org.ssgproject.content_rule_file_ownership_library_dirs
Result	pass
Title	Verify that System Executables Have Restrictive Permissions
Rule	xccdf_org.ssgproject.content_rule_file_permissions_binary_dirs
Result	pass
Title	Verify that Shared Library Files Have Restrictive Permissions
Rule	xccdf_org.ssgproject.content_rule_file_permissions_library_dirs
[5] 0:s	udo* "rocky8-disa-stig" 15:16 11-Jun-22

E produrrà un rapporto HTML:

Evaluation target	awp-hub-rocky8.network	CPE Platforms	Addresses
Benchmark URL	#scap_org.open-scap_comp_ssg-rl8-xccdf- 1.2.xml	• срелопоскульску.	 IPV4 127.0.0.1 IPV4 192.168.100.254 IPV4 172.17.0.1 IPV4 172.0.6
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHE 8		 IPV6 IPV6 0:0:0:0:0:0:0:0:1 IPV6 fe80:0:0:5054:ff:fefb:f78 IPV6 fe80:0:0:0:0:0:483:b16c:8Ef2:c2ad
Benchmark version	0.1.60		MAC 00:00:00:00:00:00 MAC 52:54:00:FB:0F:78 MAC 00:40:40:73:40:10
Profile ID	xccdf_org.ssgproject.content_profile_stig		• MAC 02;42:AC:73;4D;1C
Started at	2022-08-26T15:37:04-05:00		
Finished at	2022-08-26T15:38:20-05:00		
Performed by	root		
Test system	cpe:/a:redhat:openscap:1.3.6		
Compli The target s Rule res	ance and Scoring system did not satisfy the conditions of 243 ru ults	I es! Please review rule results a	nd consider applying remediation.
	111 passed	243	failed 7
•	ff-ll-d-milae		

3.3 Generazione di script Bash di Riparazione

Successivamente, genereremo una scansione e useremo i risultati della scansione per generare uno script bash per rimediare al sistema in base al profilo DISA stig. Non consiglio di utilizzare la riparazione automatica, è sempre necessario rivedere le modifiche prima di eseguirle.

1) Generare una scansione del sistema:

```
```bash
sudo oscap xccdf eval --results disa-stig-scan.xml --profile stig /usr/share/
xml/scap/ssg/content/ssg-rl8-ds.xml
```
```

2) Utilizzare l'output della scansione per generare lo script:

```
```bash
sudo oscap xccdf generate fix --output draft-disa-remediate.sh --profile stig
disa-stig-scan.xml
```

Lo script risultante includerà tutte le modifiche da apportare al sistema.

#### Attenzione

Esaminate questo documento prima di eseguirlo! Apporterà modifiche significative al sistema.

```
Ð
 Q
 root@awp-hub-rocky8:~/tmp
 ×
inactivity_timeout_value='900'
readarray -t SETTINGSFILES < <(grep -r "\\[org/gnome/desktop/session\\]" "/etc/dconf/db/" | grep -v 'dis
DCONFFILE="/etc/dconf/db/local.d/00-security-settings"
DBDIR="/etc/dconf/db/local.d"
mkdir -p "${DBDIR}"
if ["${#SETTINGSFILES[@]}" -eq 0]
then
 [! -z ${DCONFFILE}] || echo "" >> ${DCONFFILE}
 printf '%s\n' "[org/gnome/desktop/session]" >> ${DCONFFILE}
 printf '%s=%s\n' "idle-delay" "uint32 ${inactivity_timeout_value}" >> ${DCONFFILE}
 escaped_value="$(sed -e 's/\\/\\\/g' <<< "uint32 ${inactivity_timeout_value}")"</pre>
 if grep -q "^\\s*idle-delay\\s*=" "${SETTINGSFILES[@]}"
 sed -i "s/\\s*idle-delay\\s*=\\s*.*/idle-delay=${escaped_value}/g" "${SETTINGSFILES[@]}"
 sed -i "\\\\[org/gnome/desktop/session\\]|a\\idle-delay=${escaped_value}" "${SETTINGSFILES[@]}"
dconf update
Check for setting in any of the DConf db directories
LOCKFILES=$(grep -r "^/org/gnome/desktop/session/idle-delay$" "/etc/dconf/db/" | grep -v 'distro\|ibus'
cut -d":" -f1)
LOCKSFOLDER="/etc/dconf/db/local.d/locks"
mkdir -p "${LOCKSFOLDER}"
if [[-z "${LOCKFILES}"]]
then
 echo "/org/gnome/desktop/session/idle-delay" >> "/etc/dconf/db/local.d/locks/00-security-settings-lo
dconf update
 669,1
 1%
```

#### 3.4 Generazione dei Playbook Ansible di Riparazione

È anche possibile generare azioni di rimedio in formato playbook ansible. Ripetiamo la sezione precedente, ma questa volta con l'output di Ansible:

1) Generare una scansione del sistema:

```
```bash
sudo oscap xccdf eval --results disa-stig-scan.xml --profile stig /usr/share/
xml/scap/ssg/content/ssg-rl8-ds.xml
...
```

2) Utilizzare l'output della scansione per generare lo script:

```
```bash
sudo oscap xccdf generate fix --fix-type ansible --output draft-disa-
remediate.yml --profile stig disa-stig-scan.xml
```

#### Attenzione

Anche in questo caso, rivedetelo prima di eseguirlo! Percepite uno schema? Questa fase di verifica di tutte le procedure è molto importante!

```
Ð
 Q
 root@awp-hub-rocky8:~/tmp
 # Profile Description:
This profile contains configuration checks that align to the
In addition to being applicable to Red Hat Enterprise Linux 8, DISA recognizes this
configuration baseline as applicable to the operating system tier of
- Red Hat Enterprise Linux Server
 - Red Hat Enterprise Linux Workstation and Desktop
#
Profile ID: xccdf_org.ssgproject.content_profile_stig
Benchmark ID: xccdf_org.ssgproject.content_benchmark_RHEL-8
Benchmark Version: 0.1.60
This file was generated by OpenSCAP 1.3.6 using:
$ oscap xccdf generate fix --profile xccdf_org.ssgproject.content_profile_stig --fix-type ansible xccd
f-file.xml
It attempts to fix every selected rule, even if the system is already compliant.
How to apply this Ansible Playbook:
 $ ansible-playbook -i "localhost," -c local playbook.yml
$ ansible-playbook -i inventory.ini playbook.yml
 hosts: all
 vars:
 var_system_crypto_policy: !!str FIPS
 inactivity_timeout_value: !!str 900
 var_sudo_timestamp_timeout: !!str 0
 login_banner_text: !!str ^(You[\s\n]+are[\s\n]+accessing[\s\n]+a[\s\n]+U\.S\.[\s\n]+Government[\s\n]
"draft-disa-remediate.yml" 29907L, 1050440C
 29,1
 qoT
```

#### 3.5 Informazioni sull'Autore

Scott Shinn è il CTO di Atomicorp e fa parte del team Rocky Linux Security. Dal 1995 si occupa di sistemi informativi federali presso casa Bianca, del Dipartimento della Difesa e dell'Intelligence Community dal 1995. Parte di questo è stata la creazione degli STIG e l'obbligo di usarli e mi dispiace molto per questo.

- 31/46 -

# 4. Introduzione

Nella prima parte di questa serie, abbiamo spiegato come costruire il nostro server web con la STIG RHEL8 DISA di base applicata e, nella seconda parte, abbiamo imparato a testare la conformità STIG con lo strumento OpenSCAP. Ora faremo qualcosa con il sistema, costruendo una semplice applicazione web e applicando la STIG del server web DISA: https://www.stigviewer.com/stig/web\_server/

Per prima cosa confrontiamo ciò che stiamo affrontando: la STIG DISA di RHEL 8 è indirizzata a una piattaforma molto specifica, quindi i controlli sono abbastanza facili da capire in quel contesto, da testare e da applicare. Le STIG delle applicazioni devono essere portabili su più piattaforme, quindi il contenuto qui presente è generico per funzionare su diverse distribuzioni Linux (RHEL, Ubuntu, SuSE, ecc.)\*\*. Strumenti come OpenSCAP non ci aiutano a verificare/recuperare la configurazione. Andremo a farlo manualmente. Questi STIG sono:

- Apache 2.4 V2R5 Server; che si applica al server web stesso
- Apache 2.4 V2R5 Sito; Che si applica all'applicazione web/sito web

Per la nostra guida, creeremo un semplice server web che non fa altro che servire contenuti statici. Possiamo usare le modifiche apportate qui per creare un'immagine di base, che potremo poi usare quando costruiremo server web più complessi.

# 4.1 Avvio rapido del server Apache 2.4 V2R5

Prima di iniziare, è necessario fare riferimento alla Parte 1 e applicare il profilo di sicurezza DISA STIG. Considerate questo passo 0.

```
1.) Installare apache e mod_ssl
```

dnf install httpd mod\_ssl

#### 2.) Modifiche alla configurazione

```
sed -i 's/^\([^#].*\)**/# \1/g' /etc/httpd/conf.d/welcome.conf
dnf -y remove httpd-manual
```

```
dnf -y install mod_session
echo "MaxKeepAliveRequests 100" > /etc/httpd/conf.d/disa-apache-stig.conf
echo "SessionCookieName session path=/; HttpOnly; Secure;" >> /etc/httpd/
conf.d/disa-apache-stig.conf
echo "Session On" >> /etc/httpd/conf.d/disa-apache-stig.conf
echo "SessionMaxAge 600" >> /etc/httpd/conf.d/disa-apache-stig.conf
echo "SessionCryptoCipher aes256" >> /etc/httpd/conf.d/disa-apache-stig.conf
echo "Timeout 10" >> /etc/httpd/conf.d/disa-apache-stig.conf
echo "TraceEnable 0ff" >> /etc/httpd/conf.d/disa-apache-stig.conf
echo "RequestReadTimeout 120" >> /etc/httpd/conf.d/disa-apache-stig.conf
```

```
sed -i "s/^#LoadModule usertrack_module/LoadModule usertrack_module/g" /etc/
httpd/conf.modules.d/00-optional.conf
sed -i "s/proxy_module/#proxy_module/g" /etc/httpd/conf.modules.d/00-proxy.conf
sed -i "s/proxy_ajp_module/#proxy_ajp_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_balancer_module/#proxy_balancer_module/g" /etc/httpd/
conf.modules.d/00-proxy.conf
sed -i "s/proxy_ftp_module/#proxy_ftp_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_http_module/#proxy_http_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_connect_module/#proxy_connect_module/g" /etc/httpd/
conf.modules.d/00-proxy.conf
```

3.) Aggiornare i criteri del firewall e avviare httpd

```
firewall-cmd --zone=public --add-service=https --permanent
firewall-cmd --zone=public --add-service=https
firewall-cmd --reload
systemctl enable httpd
systemctl start httpd
```

#### 4.2 Panoramica dei Controlli Dettagliati

Se siete arrivati fin qui, probabilmente siete interessati a saperne di più su ciò che la STIG vuole che facciamo. Aiuta a capire l'importanza del controllo e come si applica all'applicazione. A volte il controllo è tecnico (cambiare l'impostazione X in Y); altre volte è operativo (come lo si usa). In generale, un controllo tecnico è qualcosa che si può modificare con il codice, mentre un controllo operativo probabilmente no.

#### 4.2.1 Livelli

- Cat I (ALTO) 5 Controlli
- Cat II (MEDIO) 41 Controlli
- Cat III (BASSO) 1 Controlli

#### 4.2.2 Tipi

- Tecnico 24 controlli
- Operativo 23 controlli

In questo articolo non tratteremo il "perché" di queste modifiche; discuteremo di ciò che deve accadere se si tratta di un controllo tecnico. Se non c'è nulla da modificare, come nel caso di un controllo Operational, il campo **Fix:** sarà vuoto. La buona notizia in molti di questi casi è che questa è già l'impostazione predefinita in Rocky Linux 8, quindi non è necessario cambiare nulla.

#### 4.3 Apache 2.4 V2R5 - Dettagli del Server

**(V-214248**) Le directory, le librerie e i file di configurazione delle applicazioni del server Web Apache devono essere accessibili solo agli utenti privilegiati.

Severity: Cat I HighType: OperationalFix: Nessuno, controlla che solo gli utenti privilegiati possano accedere ai file del server web

**(V-214242)** Il server web Apache deve fornire opzioni di installazione per escludere l'installazione di documentazione, codice di esempio, applicazioni di esempio ed esercitazioni.

Severity: Cat I High Type: Technical Fix:

sed -i 's/^\([^#].\*\)/# \1/g' /etc/httpd/conf.d/welcome.conf

**(V-214253)** Il server Web Apache deve generare un ID di sessione utilizzando la maggior parte possibile del set di caratteri per ridurre il rischio di brute force.

Severity: Cat I HighType: TechnicalFix: Nessuno, corretto per impostazione predefinita in Rocky Linux 8

**(V-214273**) Il software del server Web Apache deve essere una versione supportata dal fornitore.

Severity: Cat I HighType: TechnicalFix: Nessuno, corretto per impostazione predefinita in Rocky Linux 8

**(V-214271)** L'account utilizzato per eseguire il server Web Apache non deve avere una shell e una password di accesso valide.

Severity: Cat I HighType: TechnicalFix: Nessuno, corretto per impostazione predefinita in Rocky Linux 8

**(V-214245)** Il server web Apache deve avere il Web Distributed Authoring (WebDAV) disabilitato.

Severity: Cat II Medium Type: Technical Fix:

sed -i 's/^\([^#].\*\)/# 1/g' /etc/httpd/conf.d/welcome.conf

**(V-214264)** Il server Web Apache deve essere configurato per integrarsi con l'infrastruttura di sicurezza dell'organizzazione.

Severity: Cat II MediumType: OperationalFix: Nessuno, inoltrare i log del server web al SIEM

**(V-214243)** Il server Web Apache deve avere le mappature delle risorse impostate per disabilitare il servizio di alcuni tipi di file.

Severity: Cat II MediumType: TechnicalFix: Nessuno, corretto per impostazione predefinita in Rocky Linux 8

**(V-214240)** Il server web Apache deve contenere solo i servizi e le funzioni necessarie al funzionamento.

Severity: Cat II Medium Type: Technical Fix:

```
dnf remove httpd-manual
```

**(V-214238)** I moduli di espansione devono essere completamente rivisti, testati e firmati prima di poter esistere su un server web Apache di produzione.

Severity: Cat II Medium Type: Operational Fix: Nessuno, disattivare tutti i moduli non necessari per l'applicazione

**(V-214268)** I cookie scambiati tra il server Web Apache e il client, come i cookie di sessione, devono avere le proprietà dei cookie impostate in modo da impedire agli script lato client di leggere i dati dei cookie.

Severity: Cat II Medium Type: Technical Fix:

```
dnf install mod_session
echo "SessionCookieName session path=/; HttpOnly; Secure;" >> /etc/httpd/
conf.d/disa-apache-stig.conf
```

**(V-214269)** Il server web Apache deve rimuovere tutti i cifrari di esportazione per proteggere la riservatezza e l'integrità delle informazioni trasmesse.

Severity: Cat II MediumType: TechnicalFix: Nessuno, corretto per impostazione predefinita in Rocky Linux 8 Profilo di sicurezza DISA STIG

**(V-214260)** Il server web Apache deve essere configurato per disconnettere o disabilitare immediatamente l'accesso remoto alle applicazioni ospitate.

Severity: Cat II MediumType: OperationalFix: Nessuna, si tratta di una procedura per arrestare il server web

**(V-214249)** Il server web Apache deve separare le applicazioni ospitate dalla funzionalità di gestione del server web Apache ospitato.

Severity: Cat II MediumType: OperationalFix: Nessuno, questo è relativo alle applicazioni web piuttosto che al server

**(V-214246)** Il server Web Apache deve essere configurato per utilizzare un indirizzo IP e una porta specifici.

Severity: Cat II MediumType: OperationalFix: Nessuno, il server web deve essere configurato per ascoltare solo su un IP/ port specifico

**(V-214247)** Gli account del server web Apache che accedono all'albero delle directory, alla shell o ad altre funzioni e utilità del sistema operativo devono essere solo account amministrativi.

Severity: Cat II MediumType: OperationalFix: Nessuno, tutti i file e le directory serviti dal server web devono essere di proprietà degli utenti amministrativi e non dell'utente del server web.

**(V-214244)** Il server Web Apache deve consentire la rimozione dei mapping agli script inutilizzati e vulnerabili.

Severity: Cat II Medium
Type: Operational
Fix: Nessuno, qualsiasi cgi-bin o altre mappature Script/ScriptAlias non utilizzate devono essere rimosse

**(V-214263)** Il server web Apache non deve impedire la possibilità di scrivere il contenuto di un record di registro specificato su un server di registro di audit.

Severity: Cat II Medium
Type: Operational
Fix: Nessuno, collaborare con l'amministratore del SIEM per consentire la possibilità di scrivere il contenuto specificato dei record di registro su un server di registro di audit.

**(V-214228)** Il server web Apache deve limitare il numero di richieste di sessione simultanee consentite.

Severity: Cat II Medium Type: Technical Fix:

echo "MaxKeepAliveRequests 100" > /etc/httpd/conf.d/disa-apache-stig.conf

**(V-214229)** Il server web Apache deve eseguire la gestione della sessione lato server.

Severity: Cat II Medium Type: Technical Fix:

sed -i "s/^#LoadModule usertrack\_module/LoadModule usertrack\_module/g" /etc/ httpd/conf.modules.d/00-optional.conf

**(V-214266)** Il server web Apache deve vietare o limitare l'uso di porte, protocolli, moduli e/o servizi non sicuri o non necessari.

Severity: Cat II Medium Type: Operational Fix: Nessuno, Assicurarsi che il sito web applichi l'uso delle porte conosciute da IANA per HTTP e HTTPS.

(V-214241) Il server Web Apache non deve essere un server proxy.

# Severity: Cat II Medium Type: Technical

#### Fix:

```
sed -i "s/proxy_module/#proxy_module/g" /etc/httpd/conf.modules.d/00-proxy.conf
sed -i "s/proxy_ajp_module/#proxy_ajp_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_ftp_module/#proxy_ftp_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_http_module/#proxy_ftp_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_http_module/#proxy_http_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_connect_module/#proxy_connect_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
```

**(V-214265)** Il server Web Apache deve generare record di log che possono essere mappati al Tempo Universale Coordinato (UTC)\*\* o al Tempo Medio di Greenwich (GMT), con una granularità minima di un secondo.

Severity: Cat II MediumType: TechnicalFix: Nessuno, corretto per impostazione predefinita in Rocky Linux 8

**(V-214256)** I messaggi di avviso e di errore visualizzati ai client devono essere modificati per minimizzare l'identità del server web Apache, delle patch, dei moduli caricati e dei percorsi delle directory.

Severity: Cat II MediumType: OperationalFix: Utilizzare la direttiva "ErrorDocument" per abilitare pagine di errore personalizzate per i codici di stato HTTP 4xx o 5xx.

**(V-214237)** È necessario eseguire il backup dei dati e dei record di registro del server Web Apache su un sistema o un supporto diverso.

Severity: Cat II MediumType: OperationalFix: Nessuna, documentare le procedure di backup del server web

**(V-214236)** Le informazioni di registro del server web Apache devono essere protette da modifiche o cancellazioni non autorizzate.

Severity: Cat II MediumType: OperationalFix: Nessuna, documentare le procedure di backup del server web

**(V-214261)** Gli account non privilegiati sul sistema di hosting devono accedere alle informazioni e alle funzioni rilevanti per la sicurezza del server web Apache solo attraverso un account amministrativo separato.

Severity: Cat II MediumType: OperationalFix: Nessuno, Limitare l'accesso allo strumento di amministrazione web solo all'Amministratore di sistema, al Web Manager o a chi ne fa le veci.

**(V-214235)** I file di registro del server Web Apache devono essere accessibili solo da utenti privilegiati.

Severity: Cat II Medium

Type: Operational

**Fix:** Nessuno, Per proteggere l'integrità dei dati acquisiti nei file di registro, assicurarsi che solo i membri del gruppo Auditori, gli Amministratori e l'utente assegnato all'esecuzione del software del server Web ricevano l'autorizzazione a leggere i file di registro.

**(V-214234)** Il server web Apache deve utilizzare un meccanismo di registrazione configurato per avvisare il responsabile della sicurezza del sistema informativo (ISSO) e l'amministratore di sistema (SA) in caso di errori di elaborazione.

Severity: Cat II Medium

Type: Operational

**Fix:** Nessuno, collaborare con l'amministratore del SIEM per configurare un avviso quando non vengono ricevuti dati di audit da Apache in base alla pianificazione delle connessioni definita.

**(V-214233)** Un server Web Apache, dietro un bilanciatore di carico o un server proxy, deve produrre record di registro contenenti le informazioni IP del client

come origine e destinazione e non le informazioni IP del bilanciatore di carico o del proxy per ogni evento.

Severity: Cat II Medium

Type: Operational

**Fix:** Nessuno, accedere al server proxy attraverso il quale viene passato il traffico web in entrata e configurare le impostazioni per passare il traffico web al server web Apache in modo trasparente.

Fare riferimento a https://httpd.apache.org/docs/2.4/mod/mod\_remoteip.html per ulteriori informazioni sulle opzioni di registrazione in base alla configurazione del proxy/bilanciamento del carico.

(V-214231) Il server web Apache deve avere la registrazione di sistema abilitata.

Severity: Cat II MediumType: TechnicalFix: Nessuno, corretto per impostazione predefinita in Rocky Linux 8

**(V-214232)** Il server web Apache deve generare, come minimo, registrazioni di log per l'avvio e l'arresto del sistema, l'accesso al sistema e gli eventi di autenticazione del sistema.

Severity: Cat II MediumType: TechnicalFix: Nessuno, corretto per impostazione predefinita in Rocky Linux 8

**(V-214251)** I cookie scambiati tra il server web Apache e il client, come i cookie di sessione, devono avere impostazioni di sicurezza che impediscano l'accesso ai cookie al di fuori del server web Apache e dell'applicazione ospitata.

Severity: Cat II Medium Type: Technical Fix:

echo "Session On" >> /etc/httpd/conf.d/disa-apache-stig.conf

**(V-214250)** Il server web Apache deve invalidare gli identificatori di sessione al momento del logout dell'utente dell'applicazione ospitata o al termine di un'altra sessione.

Severity: Cat II Medium Type: Technical Fix:

echo "SessionMaxAge 600" >> /etc/httpd/conf.d/disa-apache-stig.conf

**(V-214252)** Il server Web Apache deve generare un ID di sessione sufficientemente lungo da non poter essere indovinato con la forza bruta.

Severity: Cat II Medium Type: Technical Fix:

echo "SessionCryptoCipher aes256" >> /etc/httpd/conf.d/disa-apache-stig.conf

**(V-214255)** Il server web Apache deve essere regolato per gestire i requisiti operativi dell'applicazione ospitata.

Severity: Cat II Medium Type: Technical Fix:

echo "Timeout 10" >> /etc/httpd/conf.d/disa-apache-stig.conf

**(V-214254)** Il server web Apache deve essere costruito in modo da fallire in uno stato sicuro noto se l'inizializzazione del sistema fallisce, lo spegnimento fallisce o le interruzioni falliscono.

Severity: Cat II MediumType: OperationalFix: Nessuno, Preparare la documentazione per i metodi di ripristino di emergenza per il server web Apache 2.4 in caso di necessità di rollback.

**(V-214257)** Le informazioni di debug e di tracciamento utilizzate per la diagnosi del server web Apache devono essere disattivate.

```
Severity: Cat II Medium
Type: Technical
Fix:
```

echo "TraceEnable Off" >> /etc/httpd/conf.d/disa-apache-stig.conf

**(V-214230)** Il server Web Apache deve utilizzare la crittografia per proteggere l'integrità delle sessioni remote.

Severity: Cat II Medium Type: Technical Fix:

```
sed -i "s/^#SSLProtocol.*/SSLProtocol -ALL +TLSv1.2/g" /etc/httpd/conf.d/
ssl.conf
```

**(V-214258)** Il server web Apache deve impostare un timeout di inattività per le sessioni.

Severity: Cat II Medium Type: Technical Fix:

echo "RequestReadTimeout 120" >> /etc/httpd/conf.d/disa-stig-apache.conf

**(V-214270)** Il server web Apache deve installare gli aggiornamenti software rilevanti per la sicurezza entro il periodo di tempo configurato e indicato da una fonte autorevole (ad esempio, IAVM, CTO, DTM e STIG).

Severity: Cat II MediumType: OperationalFix: Nessuno, Installare la versione corrente del software del server web e mantenere i service pack e le patch appropriate.

**(V-214239)** Il server web Apache non deve eseguire la gestione degli utenti per le applicazioni ospitate.

Severity: Cat II MediumType: TechnicalFix: Nessuno, corretto per impostazione predefinita in Rocky Linux 8

**(V-214274)** I file htpasswd del server web Apache (se presenti) devono riflettere la proprietà e i permessi corretti.

Severity: Cat II Medium
Type: Operational
Fix: Nessuno, Assicurarsi che l'account SA o Web Manager sia proprietario del file
"htpasswd". Assicurarsi che le autorizzazioni siano impostate su "550".

**(V-214259)** Il server web Apache deve limitare le connessioni in entrata da zone non sicure.

Severity: Cat II MediumType: OperationalFix: Nessuno, Configurare il file "http.conf" per includere le restrizioni.

Esempio:

Require not ip <mark>192</mark>.168.205 Require not host phishers.example.com

**(V-214267)** Il server Web Apache deve essere protetto dall'arresto da parte di un utente non privilegiato.

Severity: Cat II MediumType: TechnicalFix: Nessuno, corretto per impostazione predefinita in Rocky Linux 8

**(V-214262)** Il server Web Apache deve utilizzare un meccanismo di registrazione configurato in modo da allocare una capacità di memorizzazione dei record di registro sufficientemente grande da soddisfare i requisiti di registrazione del server Web Apache.

Severity: Cat II MediumType: OperationalFix: Nessuno, collaborare con l'amministratore del SIEM per determinare se il

SIEM è configurato per allocare una capacità di archiviazione dei record di registro sufficientemente grande da soddisfare i requisiti di registrazione del server web Apache.

**(V-214272)** Il server web Apache deve essere configurato in conformità con le impostazioni di sicurezza basate sulla configurazione di sicurezza del DoD o sulla guida all'implementazione, comprese le STIG, le guide di configurazione dell'NSA, le CTO e i DTM.

Severity: Cat III Low Type: Operational Fix: Nessuna

#### 4.4 Informazioni sull'autore

Scott Shinn è il CTO per Atomicorp e fa parte del team Rocky Linux Security. Dal 1995 si occupa di sistemi informativi federali presso la Casa Bianca, il Dipartimento della Difesa e l'Intelligence Community. Parte di questo è stata la creazione degli STIG e l'obbligo di usarli, e mi dispiace molto per questo. https://docs.rockylinux.org/