

DISA STIG On Rocky Linux 8 (Ukrainian version)

A book from the Documentation Team

Version : 2024/04/29

Rocky Documentation Team

Copyright © 2023 The Rocky Enterprise Software Foundation

Table of contents

1. Licence	3
2. ЯК: STIG Rocky Linux 8 Fast - Частина 1	4
2.1 Термінологічний довідник	4
2.2 Вступ	4
2.2.1 Крок 1: Створіть віртуальну машину	4
2.2.2 Крок 2. Завантажте Rocky Linux 8 DVD ISO	5
2.2.3 Крок 3. Завантажте інсталятор	7
2.2.4 Крок 4: СПОЧАТКУ виберіть Розбиття	7
2.2.5 Крок 5: Налаштуйте програмне забезпечення для свого середовища: встановлення сервера без граф інтерфейсу користувача	ічного 13
2.2.6 Крок 6: Виберіть профіль безпеки	14
2.2.7 Крок 7. Натисніть «Done» та перейдіть до остаточного налаштування	17
2.2.8 Крок 8. Створіть обліковий запис користувача та призначте цього користувача адміністратором	17
2.2.9 Крок 9. Натисніть «Done», а потім «Begin Installation»	19
2.2.10 Крок 10. Після завершення встановлення натисніть «Reboot System»	20
2.2.11 Крок 11: Увійдіть у свою систему STIG'd Rocky Linux 8	21
2.3 Про автора	22
3. Вступ	23
3.1 Список профілів безпеки	23
3.2 Аудит відповідності DISA STIG	25
3.3 Створення сценаріїв Bash для виправлення	27
3.4 Створення підручників щодо виправлення	29
3.5 Про автора	31
4. Вступ	32
4.1 Apache 2.4 V2R5 Server Quickstart	32
4.2 Детальний огляд елементів керування	33
4.2.1 Рівні	34
4.2.2 Типи	34
4.3 Apache 2.4 V2R5 – Інформація про сервер	34
4.4 Про автора	43

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. ЯК: STIG Rocky Linux 8 Fast - Частина 1

2.1 Термінологічний довідник

- DISA Агентство оборонних інформаційних систем
- RHEL8 Red Hat Enterprise Linux 8
- STIG Посібник із безпечного технічного впровадження
- SCAP протокол автоматизації безпечного вмісту
- DoD Міністерство оборони

2.2 Вступ

У цьому посібнику ми розповімо, як застосувати DISA STIG для RHEL8 для нової інсталяції Rocky Linux 8. Оскільки серія складається з багатьох частин, ми також розповімо, як перевірити відповідність STIG, адаптувати параметри STIG і застосувати інший вміст STIG у цьому середовищі.

Rocky Linux — це похідна від RHEL, і тому вміст, опублікований для DISA RHEL8 STIG, є однаковим для обох операційних систем. Навіть краща новина: застосування параметрів STIG вбудовано в інсталятор Rocky Linux 8 anaconda в розділі «Профілі безпеки». Під капотом усе це працює за допомогою інструменту під назвою OpenSCAP, який дозволяє вам налаштувати систему на сумісність із DISA STIG (швидко!), а також перевірити відповідність системи після встановлення.

Я буду робити це на віртуальній машині у своєму середовищі, але все тут буде застосовано точно так само на чистому залізі.

2.2.1 Крок 1: Створіть віртуальну машину

- Пам'ять 2G
- диск 30G
- 1 ядро

							rocky8-disa-stig on QEMU/KVM		- 1	×
File	Virtual M	achine	Viev	v Se	nd Key					
	8	•			•	ē				٠
	Overview				Deta	ils	KML			
	OS inforn	nation			Basic I	Details				
	Performa	ince			Nam	ne:	rocky8-disa-stig			
	Memory				11111) .	af821189_7946_42d7_h124_hdfh1h9a690f			
30	Boot Opti	ons			State	us:	Running (Booted)			
	VirtlO Dis	sk1			Title					
0	SATA CDF	ROM 1			- nue					
9	NIC :95:d	6:5b			Deso	ription				
	Tablet									
۲	Mouse									
2	Keyboard	 			Hyper	visor D	tails			
	Display S	pice			Нуре	ervisor:	KVM			
	Sound ich	19			Arch	itectur	: x86_64			
	Serial 1				Emu	lator:	/usr/bin/qemu-system-x86_64			
	Channel	lemu-g	а		Chip	set:	Q35			
	Video Vir	pice			Firm	iware:	BIOS			
	Controlle	r USB 0								
	Controlle	r SATA	0							
	Controlle	r PCle ()							
	Controlle	r VirtlO	Serial	10						
Ŷ	USB Redi	rector 1								
۲	USB Redi	rector 2								
	RNG /dev	/urando	om							
L	Add Ha	ardware						Cancel		

2.2.2 Крок 2. Завантажте Rocky Linux 8 DVD ISO

Download Rocky Linux DVD. **Примітка.** Мінімальний ISO не містить вмісту, необхідного для застосування STIG для Rocky Linux 8, вам потрібно використовувати DVD або мережеву установку.

	Download th R	Downloads e official release of Rocky Linux from of trusted mirrors. ocky Linux 8 (Current) Planned EOL: May 31 2029	one 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	Prevention	Report Bug

2.2.3 Крок 3. Завантажте інсталятор

				rocky8-disa-stig on QEM	U/KVM	<u></u> -2	• ×
File	Virtual Machine	View Send Ke	ey				
	💡 🕨	II 🔳 🔻	6				÷
					ROCKY LINUX & INSTALL	ΔΤΙΟΝ	
						Help!	
	\sim					1	
			WELCOME 1	TO ROCKY LINUX 8.			
			What language v	would you like to use during the inst	allation process?		
			English	English 🕽	English (United States)		
			Afrikaans	Afrikaans	English (United Kingdom)		
			አማርኛ	Amharic	English (India)		
	10. Silan		العربية	Arabic	English (Australia)		
	二		অসমীয়া	Assamese	English (Canada)		
			Asturianu	Asturian	English (Denmark)		
			Беларуская	Belarusian	English (Ireland)		
	\times		Български	Bulgarian	English (Nigeria)		
			বাংলা	Bangla	English (Hong Kong SAR China)		
			<u>ส</u> ัา:พา	Tibetan	English (Philippines)		
			Bosanski	Bosnian	English (Singapore)		
			Català	Catalan	English (South Africa)		
			Čeština	Czech	English (Zambia)		
			Cymraeg	Welsh	English (Zimbabwe)		
			Dansk	Neish	English (Botswana)		
				•			
					Quit	ontinue	

2.2.4 Крок 4: СПОЧАТКУ виберіть Розбиття

Це, ймовірно, найскладніший крок у встановленні та вимога дотримання вимог STIG. Вам потрібно буде розділити файлову систему операційної системи таким чином, що, ймовірно, створить нові проблеми. Іншими словами: вам потрібно точно знати, які ваші вимоги до пам'яті.

Pro-Tip

Linux дозволяє змінювати розміри файлових систем, про що ми розповімо в іншій статті. Достатньо сказати, що це одна з найбільших проблем із застосуванням DISA STIG на чистому залізі, для вирішення якої часто потрібно повне перевстановлення, тому розмір, який вам потрібен, перевищує специфікацію.



• Виберіть «Custom», а потім «Done»

INSTALLATION DESTINATION	ROCKY LINUX 8 INSTALLATION
	🖽 us
Device Selection	
Select the device(s) yourd like to install to. They will be left untouched until you click on the main	n menu's "Begin Installation" button.
Local Standard Disks	
30 GiB	
0x1af4	
vda / 30 GiB free	
Specialized & Network Disks	Disks left unselected here will not be touched.
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 <u>Refresh</u>

• Почніть додавати розділи



Схема розподілу DISA STIG для диска 30G. Я використовую простий вебсервер:

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

🧪 Pro-Tip

Налаштуйте / last i встановіть йому справді велике число, це призведе до того, що весь вільний простір на диску залишиться на /, і вам не доведеться робити жодних обчислень.

				ROCKY LINUX 8 INST	Helpi
• New Rocky Linux 8 Installation		rl-var			
/home rl-home	1024 MiB	Mount Point: /var		Device(s): 0x1af4 (vda)	
/var/log rl-var_log	4 GiB	Desired Capacity:			
/var/log/audit rl-var_log_audit	1024 MiB	10 GiB			
/var/tmp rl-var_tmp	ADD A NEW MOU	JNT POINT		Volume Group:	
SYSTEM /tmp rl-tmp	More customiza after creating th	ation options are available ne mount point below.	Encrypt	rl (4 MiB fre	e) 🕶
/var rl-var	Mount Point: Desired Capacity:	10006			
rl-swap	c	ancel Add mount point	2	Name: var	
+ - C			Note: The : be applied	Update Se settings you make on this screet until you click on the main menic Installation	
AVAILABLE SPACE 9.99 GIB TOTAL SPACE 30 GIB					
					ALL CONTRACT OF
/ Pro-Tip					
Повторення попередньої підказки про	офесіонала: НАДВИЖУ	/ЙТЕ СПЕЦИФІКАЦІЇ ва	ших файлов	их систем, навіть якщо	вам

доведеться їх розширити пізніше.

• Натисніть «Done» і «Accept Changes»

			ROCKY LINUX 8 INSTALLA
			H us
New Rocky Linux 8 Installation		rl-root	
/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		ypt (0 B free) 🕶
/ d-mont	9.51 GiB 📏	File System:	Modify
/tmp rl-tmp	1024 MiB	xfs Reformat	
/var rl-var	10 GiB		
/boot vdal	500 MiB	Label:	Name:
swap rl-swap	2 GiB		root
			Update Settings
+ – C		Note be a	: The settings you make on this screen will r applied until you click on the main menu's 'Beg
VAILABLE SPACE TOTAL SPACE LO23 KIB 30 GIB			installation ⁻ butt
l storage device selected			Rese

2.2.5 Крок 5: Налаштуйте програмне забезпечення для свого середовища: встановлення сервера без графічного інтерфейсу користувача

DATA	inux o ii	istattation					
/home rl-home			1024	MiB Mou	nt Point:	Device(s): 0x1af4 (vda)	
/var/log rl-var_log	SUMMA	ARY OF CHANGE	es es	CID		Modify	
/var/log/au	Your cu	stomizations will	result in the following ch	anges taking eff	ect after you return to the main me	nu and begin installatior	n:
rl-var_log_audi	Order	Action	Туре	Device	Mount point		1
/var/tmp	1	destroy format	Unknown	0x1af4 (vda)			
rt-var_tmp	2	create format	partition table (MSDOS)	0x1af4 (vda)			(0 B free) -
SYSTEM	3	create device	partition	vdal on Oxlaf	4		to price,
New York Control of Co	4	create format	xfs	vdal on Oxlaf	4 /boot		
rl-foot	5	create device	partition	vda2 on 0x1af	4		
/tmp	6	create format	physical volume (LVM)	vda2 on 0x1af	4		
luar	7	create device	lvmvg	rl			
/Var rl-var	8	create device	lvmlv	rl-var_log		1	
/boot	9	create format	xfs	rl-var_log	/var/log		
vdal	10	create device	lvmlv	rl-var_log_aud	it		
swap	11	create format	xfs	rl-var_log_aud	it /var/log/audit		
rl-swap	12	create device	lvmlv	rl-tmp			
				Cancel	& Return to Custom Partitioning	Accept Changes	
	10						Update Setting
					Note: 1	The settings you make o	
+ - G	4					lied until you click on th	
		_					

2.2.5 Крок 5: Налаштуйте програмне забезпечення для свого середовища: встановлення сервера без графічного інтерфейсу користувача

Це матиме значення на **кроці 6**, тому якщо ви використовуєте інтерфейс користувача або конфігурацію робочої станції, профіль безпеки буде іншим.

Done	🖽 us Hel
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 This package group allows you to share files between Linux and MS Windows(tm) systems. Debugging Tools

2.2.6 Крок 6: Виберіть профіль безпеки

Це налаштує низку параметрів безпеки в системі на основі вибраної політики, використовуючи структуру SCAP. Він змінить пакунки, які ви вибрали на **кроці 5**, додавши або видаливши необхідні компоненти. Якщо ви *вибрали* інсталяцію з графічним інтерфейсом користувача на **кроці 5**, і на цьому кроці ви використовуєте STIG без графічного інтерфейсу, це видалить графічний інтерфейс. Відрегулюйте відповідно!



Виберіть DISA STIG для Red Hat Enterprise Linux 8:

			ROCKY LINUX 8 INST/ us
Change content	Apply security policy: ON		
Choose profile belov	л. — — — — — — — — — — — — — — — — — — —		
parameters. Accordi use in U.S. National	ngly, this configuration profile is sui Security Systems.	table for	
PCI-DSS v3.2.1 Co	ntrol Baseline for Red Hat Enterp	rise Linux 8 are applied	
DISA STIG for Red This profile contains DISA STIG for Red I In addition to being configuration baseli Red Hat technologie - Red Hat Enterprise - Red Hat Enterprise - Red Hat Enterprise - Red Hat Enterprise - Red Hat Storage - Red Hat Storage - Red Hat Container DISA STIG with GU	Hat Enterprise Linux 8 configuration checks that align to t lat Enterprise Linux 8 V1R5. applicable to Red Hat Enterprise Lin e as applicable to the operating sys s that are based on Red Hat Enterp Linux Server Linux Workstation and Desktop Linux for HPC s with a Red Hat Enterprise Linux 8 Il for Red Hat Enterprise Linux 8	the ux 8, DISA recognizes this tem tier of rise Linux 8, such as: image	
TI		Select profile	
Changes that were d	one or need to be done:		
💡 No profile select	ed		

Натисніть «Select Profile» і зверніть увагу на зміни, які він збирається внести в систему. Це встановить параметри для точок монтування, додасть/видалить програми та внесе інші зміни конфігурації:

Changes that were done or need to be done:	
Package 'xorg-x11-server-Xorg' has been added to the list of excluded packages	
💡 package 'vsftpd' has been added to the list of excluded packages	
💡 package 'abrt-plugin-logger' has been added to the list of excluded packages	
💡 package 'abrt-cli' has been added to the list of excluded packages	
Package 'xorg-xll-server-utils' has been added to the list of excluded packages	
👷 package 'python3-abrt-addon' has been added to the list of excluded packages	
Changes that were done or need to be done:	

- package policycoreucits has been auteu to the list of to be installed packages

 $\ensuremath{\mathbb{G}}$ package 'usbguard' has been added to the list of to be installed packages

 $_{ar{W}}$ package 'rsyslog-gnutls' has been added to the list of to be installed packages

 $^{\odot}_{
m V}$ package 'rsyslog' has been added to the list of to be installed packages

💡 package 'firewalld' has been added to the list of to be installed packages

 \mathbb{Q} nackade 'openssi-pics11' has been added to the list of to be installed packades -

SYSTEM

Installation Destination

Custom partitioning selected

2



SOFTWARE

0

Installation Source

Local media

LOCALIZATION

Keyboard

English (US)

2.2.7 Крок 7. Натисніть «Done» та перейдіть до остаточного налаштування



2.2.8 Крок 8. Створіть обліковий запис користувача та призначте цього користувача адміністратором

У наступних посібниках ми зможемо приєднати це до корпоративної конфігурації FreeIPA. Наразі ми розглядатимемо це окремо. Зауважте, що я не встановлюю пароль root, а ми надаємо доступ нашому користувачеві за замовчуванням sudo.

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



2.2.9 Крок 9. Натисніть «Done», а потім «Begin Installation»

2.2.10 Крок 10. Після завершення встановлення натисніть «Reboot System»

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

2.2.11 Крок 11: Увійдіть у свою систему STIG'd Rocky Linux 8



Якщо все пройшло добре, ви повинні побачити тут банер із застереженням Міністерства оборони за замовчуванням.



2.3 Про автора

Скотт Шінн є технічним директором Atomicorp і є частиною команди Rocky Linux Security. Він працював із федеральними інформаційними системами Білого дому, Міністерства оборони та розвідувального співтовариства з 1995 року. Частково це було створення STIG і вимога, щоб ви їх використовували, і я дуже шкодую про це.

3. Вступ

У попередній статті ми налаштували нову систему Linux 8 із застосуванням DISA stig за допомогою OpenSCAP. Тепер ми розглянемо, як перевірити систему за допомогою тих самих інструментів, і розглянемо, які типи звітів ми можемо створювати за допомогою інструментів oscap і аналога SCAP Workbench для інтерфейсу користувача.

Rocky Linux 8 (i 9!) містить набір вмісту SCAP для тестування та виправлення відповідності проти різних стандартів. Якщо ви створили систему STIG'd у частині 1, ви вже бачили це в дії. Інсталятор anaconda використовував цей вміст, щоб змінити конфігурацію rocky 8 для впровадження різних елементів керування, встановлення/видалення пакетів і зміни способу роботи точок монтування рівня OC.

З часом ці речі можуть змінитися, і ви захочете стежити за цим. Часто я також використовую ці звіти, щоб показати доказ того, що певний контроль було реалізовано правильно. У будь-якому випадку, це запекло в Rocky. Ми почнемо з деяких основ.

3.1 Список профілів безпеки

Щоб отримати список доступних профілів безпеки, нам потрібно використати команду oscap info, яку надає пакет openscap-scanner. Це має бути вже встановлено у вашій системі, якщо ви стежите за цим, починаючи з частини 1. Щоб отримати доступні профілі безпеки:

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

🖍 Примітка

Вміст Rocky Linux 8 використовуватиме тег «rl8» у назві файлу. У Rocky 9 це буде «rl9».

Якщо все піде добре, ви повинні отримати екран, який виглядає приблизно так:

	vp-agent/src/awp-agent/active-response — ssh 192.168.122.174 Q =	×
Oocument type: Source Data Str Imported: 2022-04-29T22:32:36	eam	
Stream: scap_org.open-scap_dat Generated: (null) /ersion: 1.3 Shecklists:	astream_from_xccdf_ssg-rl8-xccdf-1.2.xml	I
Ref-Id: scap_org.open-	<pre>scap_cref_ssg-rl8-xccdf-1.2.xml</pre>	I
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)	I
Title:	Id: xccdf_org.ssgproject.content_profile_anssi_bp28_high ANSSI-BP-028 (intermediary)	I
Title:	Id: xccdf_org.ssgproject.content_profile_anssi_bp28_intermediary ANSSI-BP-028 (minimal)	I
	Id: xccdf_org.ssgproject.content_profile_anssi_bp28_minimal	
litte:	Id: xccdf org.ssgproject.content profile cis	
Title:	CIS Red Hat Enterprise Linux 8 Benchmark for Level 1 - Server	
Title:	Id: xccdf_org.ssgproject.content_profile_cis_server_ti CIS Red Hat Enterprise Linux 8 Benchmark for Level 1 - Workstation	I
Title:	CIS Red Hat Enterprise Linux 8 Benchmark for Level 2 - Workstation Id: xccdf or ssgproject.content profile cis workstation 12	I
Title:	Unclassified Information in Non-federal Information Systems and Organi	z
ations (NIST 800-171)		
Title	Id: XCCdT_org.ssgproject.content_profile_cul Australian Cyber Security Centre (ACSC) Essential Fight	
11000	Id: xccdf org.ssgproject.content profile e8	
Title:	Health Insurance Portability and Accountability Act (HIPAA)	
Title	Id: xccdf_org.ssgproject.content_profile_hipaa	
Titte:	Id: xccdf org.ssgproject.content profile ism o	
Title:	Protection Profile for General Purpose Operating Systems	
Title:	PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 8	
	Id: xccdf org.ssgproject.content profile pci-dss	
Title:	DISA STIG for Red Hat Enterprise Linux 8	
	Id: xccdf_org.ssgproject.content_profile_stig	
Title:	Id: xccdf org.ssaproject.content profile stig gui	
Referenced che	ck files:	
ssg-rl	8-oval.xml	
	system: http://oval.mitre.org/XMLSchema/oval-definitions-5	
51 0 · bash*	ProckyQ dica stig# 15-02 11 Jun 2	5
oj otbasir	TUCKy8-disa-Stig 15:02 11-JUN-2	21

DISA — це лише один із багатьох профілів безпеки, які підтримуються визначеннями Rocky Linux SCAP. У нас також є профілі для:

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

3.2 Аудит відповідності DISA STIG

Тут ε два типи на вибір:

- stig без графічного інтерфейсу
- stig_gui з графічним інтерфейсом

Запуск сканування та створення HTML-звіту для DISA STIG:

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

Це призведе до такого звіту:

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 Rule Result	<pre>Verify Permissions on /var/log Directory xccdf_org.ssgproject.content_rule_file_permissions_var_log pass</pre>
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	"rocky8-disa-stig" 15:16 11-Jun-22

I виведе звіт HTML:

Evaluation	awp-hub-rocky8.network	CPE Platforms	Addresses
Benchmark URL	#scap_org.open-scap_comp_ssg-rl8-xccdf- 1.2.xml	cpe:/o:rocky:rocky:8	 IPv4 127.0.0.1 IPv4 192.168.100.254 IPv4 172.17.0.1 IPv4 10.8.0.6
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHI 8		 IPv6 0:0:0:0:0:0:0:1 IPv6 fe80:0:0:0:5054:ff:fefb:f78 IPv6 fe80:0:0:0:0:4c83:h16c:85f2:c3ad
Benchmark version	0.1.60		 MAC 00:00:00:00:00 MAC 52:54:00:FB:0F:78
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		
Compl The target Rule res	iance and Scoring system did not satisfy the conditions of 243 ru sults	Iles! Please review rule results a	nd consider applying remediation.
·	111 passed	243	3 failed 7

3.3 Створення сценаріїв Bash для виправлення

Далі ми згенеруємо сканування, а потім використаємо результати сканування для створення сценарію bash для відновлення системи на основі профілю stig DISA. Я не рекомендую використовувати автоматичне виправлення, вам слід завжди переглядати зміни перед їх фактичним запуском.

1) Згенеруйте сканування системи:

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

2) Використовуйте цей результат сканування, щоб створити сценарій:

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

Отриманий сценарій міститиме всі зміни, які він внесе в систему.

#### Важливо

Перегляньте це, перш ніж запускати! Це внесе значні зміни в систему.

```
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</pre>
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[@]}"
 then
 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 Створення підручників щодо виправлення

Ви також можете створити дії з виправлення у форматі ansible playbook. Давайте повторимо наведений вище розділ, але цього разу з виводом ansible:

1) Згенеруйте сканування системи:

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

2) Використовуйте цей результат сканування, щоб створити сценарій:

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

🖍 Важливо

Знову ж таки, перегляньте це перед запуском! Ви відчуваєте тут закономірність? Цей етап перевірки для всіх цих процедур дуже важливий!

Ð	root@awp-hub-rocky8:~/tmp	۵		ie.		×
 **********************************	*****	:#				
# # Ansible Playbook for DISA STIG for Red H #	at Enterprise Linux 8					
# # Profile Description: # This profile contains configuration chec	ks that align to the					
# DISA STIG for Red Hat Enterprise Linux 8 # In addition to being applicable to Red H	V1R5. at Enterprise Linux 8, DISA recogniz	es this				
# configuration baseline as applicable to # Red Hat technologies that are based on F	the operating system tier of ed Hat Enterprise Linux 8, such as:					
 # - Red Hat Enterprise Linux Server # - Red Hat Enterprise Linux Workstation a # Ded Hat Enterprise Linux for HDC 	nd Desktop					
 # - Red Hat Enterprise Linux for HPC # - Red Hat Storage # - Red Hat Containers with a Red Hat Enterprise 	rprise Linux 8 image					
# # Profile ID: xccdf_org.ssgproject.conter	t_profile_stig					
<pre># Benchmark ID: xccdf_org.ssgproject.cont # Benchmark Version: 0.1.60</pre>	ent_benchmark_RHEL-8					
<pre># XCCDF Version: 1.2 # # This file was generated by OpenSCAP 1.3</pre>	6 using					
<pre># file was generated by opensex its: # \$ oscap xccdf generate fixprofile xcc f-file.xml</pre>	df_org.ssgproject.content_profile_st	igfix-	type	ansib	le xo	cd
# # This Ansible Playbook is generated from # It attempts to fix every selected rule,	an OpenSCAP profile without prelimin even if the system is already compli	ary evalı ant.	atior	I.		
# # How to apply this Ansible Playbook:						
# \$ ansible-playbook -i "localhost," -c lo # \$ ansible-playbook -i "192.168.1.155," p	cal playbook.yml laybook.yml					
<pre># \$ ansible-playbook -i inventory.ini play #</pre>	book.yml					
 ###################################	*********	:#				
- hosts: all						
<pre>vars: var_system_crypto_policy: !!str FIPS</pre>						
<pre>inactivity_timeout_value: !!str 900 var sudo timestamp timeout: !!str 0</pre>						
login_banner_text: !!str ^(You[\s\n]+a	re[\s\n]+accessing[\s\n]+a[\s\n]+U\.	S\.[\s\n]	+Gove	rnmen	t[\s\	(n]
"draft-disa-remediate.yml" 29907L, 1050440	C	2	29,1		Тс	ор

3.5 Про автора

Скотт Шінн є технічним директором Atomicorp і є частиною команди Rocky Linux Security. Він брав участь у федеральних інформаційних системах Білий дім, Міністерство оборони та розвідки з 1995 року. Частково це було створення STIG і вимоги що ви використовуєте їх, і мені дуже шкода про це.

4. Вступ

У частині 1 цієї серії ми розглянули, як створити наш веб-сервер із застосуванням базового RHEL8 DISA STIG, а в частині 2 ми дізналися, як перевірити відповідність STIG за допомогою інструменту OpenSCAP. Тепер ми збираємося зробити щось із системою, створити просту веб-програму та застосувати веб-сервер DISA STIG: https://www.stigviewer.com/stig/web_server/

Спочатку давайте порівняємо, у що ми тут втягуємося, RHEL 8 DISA STIG призначений для дуже специфічної платформи, тому елементи керування досить легко зрозуміти в цьому контексті, протестувати та застосувати. Додатки STIG мають бути переносними на кілька платформ, тому вміст тут є загальним, щоб працювати з різними дистрибутивами Linux (RHEL, Ubuntu, SuSE тощо)**. Це означає, що такі інструменти, як OpenSCAP, не допоможуть нам перевірити/виправити конфігурацію, нам доведеться робити це вручну. Ці STIG наступні:

- Apache 2.4 V2R5 сервер; що стосується самого веб-сервера
- Apache 2.4 V2R5 сайт; що стосується веб-програми/веб-сайту

Для нашого посібника ми створимо простий веб-сервер, який лише обслуговує статичний вміст. Ми можемо використати зміни, які ми вносимо тут, щоб створити базове зображення, а потім використати це базове зображення, коли пізніше створюватимемо більш складні веб-сервери.

4.1 Apache 2.4 V2R5 Server Quickstart

Перш ніж почати, вам потрібно повернутися до частини 1 і застосувати профіль безпеки DISA STIG. Вважайте це як крок 0.

1.) Встановіть apache та mod_ssl

dnf install httpd mod_ssl

2.) Зміни конфігурації

```
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 Off" >> /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/q" /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.) Оновіть політику брандмауера та запустіть 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 Детальний огляд елементів керування

Якщо ви зайшли так далеко, то, ймовірно, вам буде цікаво дізнатися більше про те, чого хоче від нас STIG. Це допомагає зрозуміти важливість елемента керування, а потім, як він застосовується до програми. Іноді елемент керування є технічним (змініть налаштування X на Y), а іноді – операційним (як ви його використовуєте). Взагалі кажучи, технічний контроль — це те, що можна змінити за допомогою коду, а оперативний контроль, ймовірно, ні.

4.2.1 Рівні

- Cat I (HIGH) 5 Controls
- Cat II (MEDIUM) 41 Controls
- Cat III (LOW) 1 Controls

4.2.2 Типи

- Technical 24 controls
- Operational 23 controls

У цій статті ми не будемо розглядати «чому» ці зміни, а лише те, що має статися, якщо це технічний контроль. Якщо ми нічого не можемо змінити, як у випадку з оперативним контролем, поле **Fix:** буде відсутнім. Хороша новина в багатьох із цих випадків, це вже за замовчуванням у Rocky Linux 8, тому вам взагалі нічого не потрібно змінювати.

4.3 Apache 2.4 V2R5 – Інформація про сервер

(V-214248) Каталоги програм веб-сервера Apache, бібліотеки та файли конфігурації мають бути доступні лише для привілейованих користувачів.

Severity: Cat I High Type: Операційний Fix: немає, перевірте, щоб лише привілейовані користувачі мали доступ до файлів веб-сервера

(V-214242) Веб-сервер Apache має надавати параметри встановлення, щоб виключити встановлення документації, зразків коду, прикладів програм і навчальних посібників.

Severity: Cat I High Type: Technical Fix:

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

(V-214253) Веб-сервер Apache має генерувати ідентифікатор сеансу, використовуючи якомога більше набору символів, щоб зменшити ризик застосування грубої сили.

Severity: Cat I High Type: технічний Fix: немає, виправлено за умовчанням у Rocky Linux 8

(V-214273) Версія програмного забезпечення веб-сервера Apache має підтримуватися постачальником.

Severity: Cat I High Type: Technical Fix: Немає, виправлено за замовчуванням у Rocky Linux 8

(V-214271) Обліковий запис, який використовується для запуску веб-сервера Apache, не повинен мати дійсну оболонку входу та визначений пароль.

Severity: Cat I High Type: Technical Fix: Немає, виправлено за замовчуванням у Rocky Linux 8

(V-214245) На веб-сервері Арасһе має бути вимкнено Web Distributed Authoring (WebDAV). **Severity:** Cat II Medium **Type:** Technical **Fix:**

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

(V-214264) Веб-сервер Apache має бути налаштований для інтеграції з інфраструктурою безпеки організації.

Severity: Cat II Medium Type: Operational Fix: Немає, пересилати журнали вебсервера до SIEM (V-214243) Веб-сервер Арасһе має мати налаштовані зіставлення ресурсів, щоб вимкнути обслуговування певних типів файлів.

Severity: Cat II Medium **Type:** Technical **Fix:** немає, виправлено за умовчанням y Rocky Linux 8

(V-214240) Веб-сервер Apache має містити лише служби та функції, необхідні для роботи.

Severity: Cat II Medium Type: Technical Fix:

dnf remove httpd-manual

(V-214238) Модулі розширення мають бути повністю перевірені, протестовані та підписані, перш ніж вони зможуть існувати на робочому веб-сервері Apache.

Severity: Cat II Medium Type: Operational Fix: Жодного, вимкнути всі непотрібні для програми модулі

(V-214268) Файли cookie, якими обмінюються веб-сервер Apache і клієнт, наприклад файли cookie ceancy, повинні мати властивості файлів cookie, налаштовані на заборону клієнтським сценаріям читати файли cookie даних.

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) Веб-сервер Apache має видалити всі шифри експорту, щоб захистити конфіденційність і цілісність переданої інформації.

Severity: Cat II Medium Type: Technical Fix: Немає, виправлено за замовчуванням у профілі безпеки Rocky Linux 8 DISA STIG

(V-214260) Веб-сервер Apache має бути налаштований на миттєве відключення або вимкнення віддаленого доступу до розміщених програм.

Severity: Cat II Medium Type: Operational Fix: Ні, це процедура зупинки вебсервера (V-214249) Веб-сервер Арасһе має відокремити розміщені програми від функцій керування веб-сервером Арасһе.

Severity: Cat II Medium Type: Operational Fix: Жодного, це стосується вебпрограм, а не сервера

(V-214246) Веб-сервер Арасһе має бути налаштований на використання вказаної IP-адреси та порту.

Severity: Cat II Medium Type: Operational Fix: Немає, веб-сервер має бути налаштований на прослуховування лише певної IP-адреси/порту

(V-214247) Облікові записи веб-сервера Apache, які мають доступ до дерева каталогів, оболонки чи інших функцій і утиліт операційної системи, мають бути лише адміністративними обліковими записами.

Severity: Cat II Medium **Type:** Operational **Fix:** Нічого, усі файли та каталоги, які обслуговує веб-сервер, мають належати адміністраторам, а не користувачу веб-сервера.

(V-214244) Веб-сервер Арасһе має дозволяти видаляти зіставлення з невикористаними та вразливими сценаріями.

Severity: Cat II Medium Type: Operational Fix: Жодного, будь-які зіставлення cgi-bin або інші зіставлення Script/ScriptAlias, які не використовуються, потрібно видалити

(V-214263) Веб-сервер Apache не повинен перешкоджати запису вказаного вмісту запису журналу на сервер журналу аудиту.

Severity: Cat II Medium Type: Operational Fix: Hi, співпрацюйте з адміністратором SIEM, щоб надати можливість записувати вказаний вміст запису журналу на сервер журналу аудиту.

(V-214228) Веб-сервер Apache має обмежити кількість дозволених одночасних запитів на сеанс.

Severity: Cat II Medium Type: Technical Fix:

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

(V-214229) Веб-сервер Арасhе має керувати сеансом на стороні сервера.

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) Веб-сервер Арасһе повинен забороняти або обмежувати використання незахищених або непотрібних портів, протоколів, модулів і/або служб.

Severity: Cat II Medium **Type:** Operational **Fix:** Hi, переконайтеся, що на вебсайті використовуються добре відомі порти IANA для HTTP та HTTPS.

(V-214241) Веб-сервер Арасhе не має бути проксі-сервером.

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_http_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) Веб-сервер Арасһе має генерувати записи журналу, які можна зіставляти з універсальним координованим часом (UTC)** або середнім часом за Гринвічем (GMT), які мають відмітку з мінімальною ступінчастістю в одну секунду.

Severity: Cat II Medium **Type:** Technical **Fix:** Немає, виправлено за замовчуванням у Rocky Linux 8

(V-214256) Попередження та повідомлення про помилки, які відображаються клієнтам, необхідно змінити, щоб мінімізувати ідентифікацію веб-сервера Apache, виправлень, завантажених модулів і шляхів до каталогу.

Severity: Cat II Medium **Type:** Operational **Fix:** Використовуйте директиву "ErrorDocument", щоб увімкнути спеціальні сторінки помилок для кодів статусу HTTP 4xx або 5xx.

(V-214237) Для даних журналу та записів із веб-сервера Apache необхідно створити резервну копію на іншій системі чи носії.

Severity: Cat II Medium Type: Operational Fix: Ні, задокументуйте процедури резервного копіювання веб-сервера

(V-214236) Інформація журналу з веб-сервера Apache повинна бути захищена від несанкціонованої зміни або видалення.

Severity: Cat II Medium Type: Operational Fix: Ні, задокументуйте процедури резервного копіювання веб-сервера

(V-214261) Непривілейовані облікові записи в системі хостингу мають мати доступ лише до інформації, що стосується безпеки веб-сервера Apache, і працювати через окремий обліковий запис адміністратора. Severity: Cat II Medium Type: Operational Fix: Немає, обмежити доступ до інструменту вебадміністрування лише для системного адміністратора, веб-менеджера або призначених веб-менеджером осіб.

(V-214235) Файли журналу веб-сервера Apache мають бути доступні лише для привілейованих користувачів.

Severity: Cat II Medium Type: Operational Fix: Немає. Щоб захистити цілісність даних, які зберігаються у файлах журналу, переконайтеся, що дозволи на читання файлів журналу мають лише члени групи аудиторів, адміністратори та користувач, призначений для запуску програмного забезпечення веб-сервера.

(V-214234) Веб-сервер Apache має використовувати механізм журналювання, налаштований на сповіщення спеціаліста з безпеки інформаційної системи (ISSO) і системного адміністратора (SA) у випадку збій обробки.

Severity: Cat II Medium Type: Operational Fix: Ні, працюйте з адміністратором SIEM, щоб налаштувати сповіщення, коли дані аудиту не надходять від Apache на основі визначеного розкладу підключень.

(V-214233) Веб-сервер Арасһе за балансувальником навантаження або проксісервером має створювати записи журналу, що містять інформацію про IPадресу клієнта як джерела та призначення, а не завантаження інформацію про IP балансера або проксі з кожною подією.

Severity: Cat II Medium **Type:** Operational **Fix:** Hi, отримати доступ до проксісервера, через який передається вхідний веб-трафік, і налаштувати параметри для прозорої передачі веб-трафіку на веб-сервер Apache.

Зверніться до https://httpd.apache.org/docs/2.4/mod/mod_remoteip.html, щоб отримати додаткову інформацію про параметри журналювання на основі налаштувань проксі/навантаження.

(V-214231) На веб-сервері Арасһе має бути ввімкнено системне журналювання.

Severity: Cat II Medium **Type:** Technical **Fix:** Немає, виправлено за замовчуванням у Rocky Linux 8

(V-214232) Веб-сервер Apache має створювати принаймні записи журналу для запуску та завершення роботи системи, доступу до системи та подій автентифікації системи.

Severity: Cat II Medium **Type:** Technical **Fix:** Немає, виправлено за замовчуванням у Rocky Linux 8

V-214251 Файли cookie, якими обмінюються веб-сервер Apache і клієнт, наприклад файли cookie ceancy, повинні мати параметри безпеки, які забороняють доступ до файлів cookie за межами вихідного веб-сервера Apache і розміщеної програми.

Severity: Cat II Medium Type: Technical Fix:

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

(V-214250) Веб-сервер Apache має робити ідентифікатори сеансу недійсними після виходу користувача розміщеної програми або іншого завершення сеансу.

Severity: Cat II Medium Type: Technical Fix:

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

(V-214252) Веб-сервер Apache має генерувати ідентифікатор сеансу достатньо довгий, щоб його неможливо було вгадати за допомогою грубої сили.

Severity: Cat II Medium Type: Technical Fix:

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

(V-214255) Веб-сервер Apache має бути налаштований відповідно до робочих вимог розміщеної програми.

Severity: Cat II Medium Type: Technical Fix:

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

(V-214254) Веб-сервер Apache має бути створений таким чином, щоб перевести його у відомий безпечний стан, якщо не вдається ініціалізувати систему, завершити роботу чи завершити роботу.

Severity: Cat II Medium Type: Operational Fix: Ні, підготуйте документацію щодо методів аварійного відновлення для веб-сервера Apache 2.4 у разі необхідності відкату.

(V-214257) Інформація про налагодження та трасування, яка використовується для діагностики веб-сервера Apache, має бути вимкнена.

Severity: Cat II Medium Type: Technical Fix:

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

(V-214230) Веб-сервер Арасһе має використовувати криптографію для захисту цілісності віддалених сеансів.

Severity: Cat II Medium Type: Technical Fix:

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

(V-214258) Веб-сервер Арасһе має встановити час очікування неактивності для сеансів.

Severity: Cat II Medium Type: Technical Fix:

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

(V-214270) Веб-сервер Арасһе має інсталювати оновлення програмного забезпечення, пов'язані з безпекою, протягом налаштованого періоду часу, указаного авторитетним джерелом (наприклад, IAVM, CTO, DTM та STIG).

Severity: Cat II Medium **Type:** Operational **Fix:** Hi, інсталюйте поточну версію програмного забезпечення веб-сервера та підтримуйте відповідні пакети оновлень і виправлень.

(V-214239) Веб-сервер Apache не повинен виконувати керування користувачами для розміщених програм.

Severity: Cat II Medium **Type:** Technical **Fix:** Немає, виправлено за замовчуванням у Rocky Linux 8

(V-214274) Файли htpasswd веб-сервера Apache (за наявності) мають відображати належне право власності та дозволи.

Severity: Cat II Medium Type: Operational Fix: Ні, переконайтеся, що обліковий запис SA або Web Manager володіє файлом "htpasswd". Переконайтеся, що для дозволів встановлено значення «550».

(V-214259) Веб-сервер Apache має обмежувати вхідні з'єднання з незахищених зон.

Severity: Cat II Medium **Type:** Operational **Fix:** Hi, налаштуйте файл "http.conf", щоб включити обмеження. Приклад:

```
Require not ip 192.168.205
Require not host phishers.example.com
```

(V-214267) Веб-сервер Apache має бути захищений від зупинки непривілейованим користувачем.

Severity: Cat II Medium Type: Technical Fix: Немає, виправлено Rocky Linux 8 за замовчуванням

(V-214262) Веб-сервер Apache повинен використовувати механізм журналювання, налаштований на виділення достатньо великої ємності для зберігання записів журналу, щоб задовольнити вимоги веб-сервера Apache до журналювання.

Severity: Cat II Medium Type: Operational Fix: немає, попрацюйте з адміністратором SIEM, щоб визначити, чи налаштовано SIEM на виділення достатньо великої ємності для зберігання записів журналу, щоб відповідати вимогам веб-сервера Apache до журналювання.

(V-214272) Веб-сервер Арасһе має бути налаштований відповідно до параметрів конфігурації безпеки на основі конфігурації безпеки Міністерства оборони або вказівок із впровадження, включаючи STIG, посібники з конфігурації NSA, СТО та DTM.

Severity: Cat III Low Type: Operational Fix: None

4.4 Про автора

Скотт Шінн є технічним директором Atomicorp і є частиною команди Rocky Linux Security. Він працював із федеральними інформаційними системами Білого дому, Міністерства оборони та розвідувального співтовариства з 1995 року. Частиною цього було створення STIG і вимога th Ви використовуєте їх, і я дуже шкодую про це. https://docs.rockylinux.org/