

## How To Guide - How to Remediate

This guide aims to assist you in starting the cyber vulnerability remediation process using the Insight portal. This tutorial assumes that you successfully managed to analyze the results of the Insight scans.

The vulnerability remediation process involves taking one of the following decisions as regards a detected vulnerability:

- Fix it by patching (often done as updating the vulnerable software)
- Fix it by decommissioning (removing the vulnerable software)
- Accept the risk of a vulnerability.
- Mark it as a False Positive.

The Insight Portal assists in the remediation process by tracking vulnerabilities and fixes, and by providing prioritized remediation plans. We recommend the following remediation flow:



1. <u>Access and implement the remediation plan</u> provided by the Insight Portal, following the next steps:

a. <u>Access the *reports* menu</u>. The menu is accessible from the options displayed on the left side of the screen.

b. <u>Access the *Remediation Report sub-tab in the*</u> <u>*Remediation tab*</u>. The tab and sub-tab are accessible from the options displayed on the top left side of the *reports* page.

c. <u>Implement the recommended actions in the provided</u> order.

The remediation actions are the best actions to take in order to reduce the largest amount of cybersecurity risk.



- infigured 🔿 🔲 🖓 🔞 🔍 🍥 🕒 Logged in to Client De Contextual Risk Scoring Repor for: File Sharing ad XLSX All devices ~ ) ( All w Qs 0 eports A Exploitable 100 CRS: High ŝ CRS: High CRS: High CRS
- 2. <u>Remediate the riskiest vulnerabilities</u> after taking the actions in the *Remediation Reports*. To achieve this:

- a. <u>Access the *reports* menu</u>. The menu is accessible from the options displayed on the left side of the screen.
- b. <u>Access the *Contextual Risk Report sub-tab from the Risk tab*</u>. The tab and sub-tab are accessible from the options displayed on the top left side of the *reports* page.
- c. <u>Click the dropdown</u> placed in front of each CVE to read and implement the remediation action written in the *Solution* section.

We recommend filtering vulnerabilities in the *Contextual Risk Report* by Criticality or by Weaponized level.

3. <u>Remediate other critical vulnerabilities.</u> To achieve this:



_	Business Contexts (14)      Back Contexts (14)      View discovered applications on your	Technical Contexts (33) Applications (1,888)	Devices	. (11)				Manage Scan	Surface
	Pitters       Image: Control         Pices enter to search       Image: Control         Image: Control       Image: Con	Aparte Apache Sonie Tomcat Concat S.32     Apache Apache Scan: Yes     Diate Scan: Yes     Diate Scan: Scan: Yes     Diate Scan: Scan: Scan: Yes     Diate Scan: Scan: Scan: Yes     Diate Scan: Scan: Scan: Yes     Open Port: 8005	Provide a constraint of the constraint of t	Apparent for a set of the se	Connect Apparents           Asache (504) 21.4.1           CP           Basche Logal 21.6.1           Di Hostaner seltcadainteiligence.com           II Hostaner seltcadainteiligence.com           II Hostaner Seltcadainteiligence.com           O IP: 20.79.218.228.61337           O Open Port: e11337 (HTTP)				
<b>(</b> )		Last Seen: 8 hours ago     Last Scanned: 8 hours ago     Critical     Urgent attention required		CPE: cpe:2.3:a:apache:http_server:2.4.3 CLast Seen: a year ago Critical Urgent attention required	CPE: cpe:2.3:a:apache:http_server:2.4.38 CLast Seen: 2 years ago Critical Urgent attention required		C FCF cpt2.3 a spech colog4 21 Alt ******* { C C Last Seen: 18 minutes ago Critical Upper lamoto negated Upper lamoto negated C Critical C Seen on Last Scan: Yes D Indearman: cristilian-fibblocal D IP 192186 685 2 C C C C cpt2.3 acticut shyconnect_secure_mobili D Last Seen: 7 hours ago C Las		
© ■ elements Aurorita Aurorita		Apscher Tomcat 8:5.32     Sein on Last Scar Ves     Hostname: split/Localintelligence.com     P: 20.79.216.228.01337     Opp Port: 61337 (HTTP)     C PC: cpc 3:33 apachet koncatil 6:5.32*******     Last Seen: 33 minutes ago     Last Gener Management	0 0	Apache Tomcal 8 8.5.22     Apache Tomcal 8 8.5.22     Seen oi Last Scan. No     Hostname: APE-ADPCoi     Hostname: APE-ADPCoi     Den Port: 8080 (HTTP)     CPE-spe3: Saspachadonce.8.5.32     CPE-spe3: Saspachadonce.8.5.32     Last Seen: 2 years ago      Moties non last scan     Import protifyed scan store in	Apache Toncat Boss Apache Toncat Bass G. Seen on Lat Son: Yes III Hostname: ADOCFTC P. Ita Bab C. CPE Cipe 2.3 angle in tomas 8.5.32******** Lat Seen & Bhours ago Lats Scanned: 8 hours ago Chicle Uppert Mandon regard	6			
S actings		Started [Apert Start     Seen on Last Scan: Yes     Seen on Last Scan: Yes     []     Hostname critisms-mbs.local     P: 102 168 & 852     CFC ge2.3 accisconvebes.meetings.4111**     Last Scener.3 anombs ago     Last Scener.3 anombs ago	O 0	Strengt Joynt Stand     Serie on Last Scan. Yes     Seen on Last Scan. Yes     Mestame: cristman: mbp local     P 102:168.06.52     Cfl:cpe2.3a.mo:3lls:frefor.278.8.0******     Last Scan.7 hours agp     Last Scan.3 months ago     Last Scan.3 months ago     Mathematical Smorths ago	G G	Control / Agent based     Microsoft Weddows Server 2019 Datacenter 64- bit 1600 Microsoft Weddows Corporation (1609)     Gen on Last Scin: Yes     Microsoft Weddows Corporation (1609)     Hostiname: APE-DomainContr     Gen Pi 192:188 253.5     GPE Cipe 2.3 aunicrosoft windows server.2019.     Get Sorten a year ago     tard Sorten a year ago	С С	Conversit / Aporters     Organing System on 192.188.0.31     G. Seen on Last Scan: Yes     Or IP 192.088.037     Or Last Seen: 4 months ago     Last Seen: 4 months ago     Concered 8 months ago     Concered 8 months ago	G

- a. <u>Access the *elements* menu</u>. The menu is accessible from the options displayed on the left side of the screen.
- b. Choose to display the vulnerabilities by <u>accessing the *Applications* tab</u>. The tab is accessible from the options displayed on the top left side of the *elements* page.

You can also access the *Devices* tab if you are interested to solve issues by device.

- c. <u>Filter by Criticality</u> using the filters on the left side of the page.
- d. <u>Click an application</u> and investigate the CVEs and the remediation actions using the table.
- e. <u>Click the CVEs</u>. A pop-up will display. <u>Use the buttons on the bottom right of the pop-up</u> to:



							Ø			
	View Taw	CVE-2019-0232	▽	Vulnerability Information						
	۵ ک				15.04.2019 4 years ago 🛈					
		Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable Remote Code Execution due to a bug in the way the JRE passes command line an	to guments		23.08.2022 0					Q.
		to Windows. The CGI Serviet is disabled by default. The CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disable								
		default in all versions in response to this vulnerability), For a detailed explanation JRE behaviour, see Markus Wulftange's blog			01.08.2023 # hours ago ①					
		(https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections- windows.html) and this archived MSDN blog			26.04.2023 3 months ago 🔿					
		(https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com tlepassagesallalke/2011/04/23/everyone-quotes-command-line-arguments-the-	1/twistylit wrong-							
				Apache Tomcat 8.5.32						
					81					
		RLE Score Exploits availa	ble		10.0					
					<u> </u>			Tomost Tomost8 to the		
		This application meets all technical prerequisites, therefore its								
		<ul> <li>exploitation is feasible in real-life. The following prerequisites were checked in your specific environment.</li> </ul>			AV:N/AC:M/Au:N/C:C/I:C/A:C					
					CWE-78					
		Exploitation Prerequisites								
		1. Tomcat is running on Windows			Active					
		N/A								
		Apache Tomcat 8.5 Tomcat8 (remove only) 8.5.32								
		3. CGI support is enabled								
				Attack Vector Information						
		4. Privileged context is enabled			LOCAL	ADJACENT NETWORK	NETWORK	osoft Windows Server 64-bit manufacturer		
		C-\Program Files (x86)\Apache Software Foundation\tomcat\conf\context.xm e 19			HOH	MEDILIM	LOW	until the patches are		
		5. EnableCmdLineArguments is enabled	N/A		MENTRIC	PINOI E	NONE			
		only applicable for Torncat 9			NONE	DADTIAL	COMPLETE			
		C:\Program Files (x86)\Apache Software Foundation(tomcat(conf)web.xml lin			NONE	DADTIAL	COMPLETE	Tomcat Tomcat® to the		
		87 7. Evoloitable files are deployed					COMPLETE			
		(C:\\Program Files (x86)\\Apache Software Foundation\\Tomcat 8.5\\webapps			NONE	NONE PARTIAL				
					* D G O		* ⊞ © O &			
		CVE-2019-10072  7.5 23.08.2022 01. 10 10 10 10 10 10 10 10 10 10 10 10 10								
		Remote,								

- i. Mark a vulnerability as active
- ii. Add a vulnerability to review.

You can access vulnerabilities added to review using the *In Review Report* sub-tab from the *Risk* tab, accessible in the *reports* menu.

iii. Mark as fixed

Vulnerabilities marked as fixed are confirmed by the Insight portal at the next scan.

- iv. Mark as a false positive
- v. Accept the risk.



-								1 configured	Ø@Q ©	Logged in to Client I	Demo1 🗸 👔 Cristian	Sandescu (Administrator) [->	
	Internal Organization     ADOCFTC												
	Scanned   Agent-based ADOCFTC	Overview	System OVAL Sci	ans Network Ec	ige Applications (150)	Associated CVEs	(31) Alerts						
	Go Agent State: online	31 Associ	iated CVEs										
	Gro Agent last check-in: a minute ago	View raw vulne	erability data of poter	itial issues discove	red on this element								
	Go Agent last update: 8 hours ago	Juliow II	ixed vullierabilities										
	◎ IP: 10.8.0.4	Edit 31 vulnera	abilities: Select	^ )( CH	ear Selection			t Type search term and press Enter Q					
	Upen Ports: 135, 49669, 800		CVE Mark as Ac	tive 🗸	Attack Vector	Discovered	Last Seen	Last State	Weaponized	Summary	Remediation	Affects	
	Business Impact: 50		Add to Rev	iew				Change				1	
	CRSS: 3401	$\odot$ $\sim$	Active Mark as fix g confirma	ed (pendin tion)									
0	Critical Urgent attention required		CVE-20 Mark as Fa	lse Positive		23.08.2022 a year ago	17.05.2023 3 months ago	17.05.2023 3 months ago	Yes	Apache Log4j2 2.0- beta9 through 2.15.0 (excluding security	Update Apache Apache Tomcat Tomcat8 to the latest	Apache Apache Tomcat Tomcat8 8.5.32 running	
	Skip Network Edge scans		Accept Ris	ĸ	Remote, unauthenticated, medium complexity				releases 2.12.2, 2.12.3, and 2.3.1)	version	on :8005		
scan surface	Scan now Edit alias Edit tags									JNDI features used in configuration, log messages, and parameters do not			
	Decommission device Delete device												
elements	Hierarchy									protect against			
	V 🕼 Internal Organization		CVE-2021-44228	• 10.0	æ	23.08.2022 a year ago	01.08.2023 8 hours ago	01.08.2023 8 hours ago	Yes	Apache Log4j2 2.0- beta9 through 2.15.0	Update Apache Tomcat Tomcat8 to the	Apache Tomcat Tomcat8 8.5.32	
reports	~ O ADOCFTC				Remote,					(excluding security releases 2.12.2,	latest version		
Ģ	V Microsoft Windows Server 2019 Datacenter 64-bit 1809 Microsoft Corporation (1809)				unauthenticated, medium complexity					2.12.3, ellu 2.3.17 JNDI features used in configuration, log messages, and parameters do not protect against			
alerts	<ul> <li>Svchost 10.0.17763.1</li> </ul>												
鐐	Spoolsv 10.0.17763.1		CVE-2020-1938	9.8		23.08.2022	01.08.2023	26.04.2023	Yes	When using the	Update Apache	- Apache Tomcat	
settings	Apache Apache Tomcat Tomcat8				(HE)					Apache JServ Protocol (AJP), care	Tomcat Tomcat8 to the latest version	Tomcat8 8.5.32	
	Docker Engine 19 03 14				Remote, unauthenticated, low complexity					must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as being bibber trust			
	O Vmms 10.0.17763.2867												
	Apache Tomcat Tomcat8 8.5.32			2-25762 🔵 8.6	Remote, unauthenticated, low complexity	23.08.2022 a year ago	01.08.2023 8 hours ago		No	If a web application sends a WebSocket message concurrently with the WebSocket connection closing when running on Anache Tomcat 8.5.0	Update Apache Tomcat Tomcat8 to the latest version	Apache Tomcat Tomcat8 8.5.32	
	Python Standard Library (64-bit) 3.8.10150.0		CVE-2022-25762					26.04.2023 3 months ago					
	Python Documentation (64-bit) 3.8.10150.0												
	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.29.30037												
	Python Development Libraries									to 8.5.75 or Apache Tomcat 9.0.0.M1 to			

4. <u>Track your remediation progress</u> using the Remediation Tracking section in the *Customer Vulnerability* 

Report, accessible in the reports menu.

