Footprint - Collaborative Remediation

An overview of CODA Footprint's remediation capabilities



CODA Footprint's new Collaborative Remediation capabilities offer a complete view of what needs to be remediated, centralized vulnerability management into a single pane of glass across security & IT operational teams, prioritization, and integrated tracking for all your vulnerability remediation workflows from detection to fix confirmation.

This set of new tools supports your IT, Security and Application teams in mitigating threats and decreasing risk by offering a complete picture across your Organizational Footprint in a friendly and collaborative way.

Vulnerability Hunting:

Empower your team with centralized vulnerability hunting capabilities, offering a complete single pane of glass view to identified vulnerabilities across your entire install base. This vulnerability centric point of view allows you to proactively assess and prioritize remediation, enhancing your organization's security resilience.

Our new Vulnerability Hunting Report focuses on specific findings and shows their occurrence frequency, current status and affected devices all-in-one screen. Once a new vulnerability is in the news simply filter and click to see if you are affected and what is the magnitude of your exposure.

			noiterine(TCD) started as hour ano											-
	^{71%} c	Cloud Scanner Analyzing n	ew data							1 configu		N 🕲 Q 🔹 🥃 🗠	gged in to FEDR 🗸	CODA Support (Administrator) [→ support@codaintelligence.com
••		vulnerability	Remediation Risk Configuration Action											
	Exect	utive Report Technical	Report Vulnerabilities Per Device Vulnerability Hun	iting										
		erability Hunting nd manage discovered vul												
														e search term and press Enter Q
	П	Vulnerability		4	CVSS Score		CVSS Impact		Attack Vector	First Care	Last Seen	Vole		Actions
	-		Summary	4	CVSS Score	Severity	CVSS Impact	CVSS Exploit	Attack vector	First Seen	Last Seen	Vulnerability States	Assets affected	
0		CVE-2014-9912	The get_Licu_disp_value_arc_php function in extintificational incodes, methods c. In PHP before 5.3.29, 5.4.x before 5.4.30, and 5.5.x before 5.5.14 does not properly restrict calls to the IcU uneshand c.pp component, which allows immole attackers to cause a component, which allows immole attackers to cause unspecified other impact value or possibly have unspecified other impact value locale_get_stippiay_name call with a long first argument.	Yes	9.8	CRITICAL	0 5.9	0 3.9	NETWORK	06.07.2023 7 months ago	31.01.2024 an hour ago	 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ 	Applications: 1 Devices: 1	#8
() ()		CVE-2015-4116	function in ext/spl/spl_heap.c in PHP before 5.5.27 and 5.6.x before 5.6.11 allows remote attackers to execute	Yes	9.8	CRITICAL	9 5.9	O 3.9	NETWORK	06.07.2023 7 months ago	31.01.2024 an hour ago	● 0 ● 0 ● 0 ● 0 ● 0 ● 0 ● 0 ● 1	Applications: 1 Devices: 1	#8
			arbitrary code by triggering a failed SplMinHeap::compare operation.											
elements		CVE-2015-4599	The SoapFault:toString method in ext/soap/soap.c In PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information, cause a denial of service	Yes	9.8	CRITICAL	9 5.9	O 3.9	NETWORK	06.07.2023 7 months ago	31.01.2024 an hour ago	● 0 ● 0 ● 0 ● 0 ● 0 ● 0 ● 0 ● 1	Applications: 1 Devices: 1	#8
reports			(application crash), or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.											
Q. alerts		CVE-2015-4600	The SoapClient implementation in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service	Yes	9.8	CRITICAL	9 5.9	O 3.9	NETWORK	06.07.2023 7 months ago	31.01.2024 an hour ago	● 0 ● 0 ● 0 ● 0 ● 0 ● 0 ● 0 ● 1	Applications: 1 Devices: 1	#B
			(application crash) or possibly execute arbitrary code via an unexpected data type, related to "type contuion" issues in the (1) SoupCilent:getLastRequest(2) SoupCilent:getLastRequestHeaders, (3) SoupCilent:getLastRequestHeaders, (4) SoupCilent:getLastRequestHeaders, (5) SoupCilent:getCookles, and (6) SoupCilent:setCookle methods.											
		CVE-2015-4601	DHD before 5.6.7 might allow remote attackers to	No	0 98	CRITICAL	A 50	A 30	NETWORK	06.072023	31 01 2024		Applications: 1	

The New Technical Report:

Introducing our all-in-one Technical Report, providing a complete view of active and closed vulnerabilities. This report offers a comprehensive overview, enabling you to identify trends, prioritize actions, and make informed decisions to strengthen your security posture. The new technical report offers a complete view of all findings and their status along with accurate first detection time, publish time and remediation time.

	71%	Critical Service Health & Cha Cloud Scanner Analy:	inge Monitoring(TCP) starte zing new data	d an hour ago	\otimes								™ 0 % [🤇)@Q ® 🥃	Logged in to FE	DR 🗸 💿 CODA S	Cupport Administrator [→
		erview Vulnerab	Remediation	on Risk Cor		on Plan											
	Exec	cutive Report Tech	nnical Report Vul	nerabilities Per Device	Vulnerability Hu	nting											
Technical Report View and analyze discovered vulnerabilities																	
	\odot	Download XLSX															
		Device Name		CVE	State	Summary	Remediation	47	0		đ	s	Attack Vector	Discovered	Published	Last Seen	Last State Changed
		ngfw.codacloud. net	40.88.131.209	CVE-2015-0204	Closed / Fix Confirmed	The ssi3_get_key_exchange function in s3_cint.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2		9 5.3	O 3.6	• 1.6	HIGH	()	18.03.2022 2 years ago	09.01.2015 9 years ago	29.03.2023 10 months ago	30,03,2023 10 months ago
Our view ever view ecan so face elements		ngfw.codacloud. net	40.88.131.209	CVE-2011-3389	Closed / Fix Confirmed	The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Expl	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.0 protocols in favor of the TLSv1.2	Yes	5 .3	3 .6	• 1.6	NONE	()	18.03.2022 2 years ago	06.09.2011 12 years ago	29.03.2023 10 months ago	30.03.2023 10 months ago
reports Q alerts)	ngfw.codacloud. net	40.88.131.209	CVE-2015-0204	Closed / Fix Confirmed	The ssi3_get_kay_exchange function in s3_cint.c in OpenSSL before 0.9.8zd, 10.0 before 10.0p, and	It is recommended to disable the deprecated TLSV1.0 and/or TLSV1.1 protocols in favor of the TLSV1.2		9 5.3	O 3.6	O 1.6	HIGH	(†)	05.06.2022 2 years ago	09.01.2015 9 years ago	30.03.2023 10 months ago	25.10.2023 3 months ago

Footprint - Collaborative Remediation

An overview of CODA Footprint's remediation capabilities

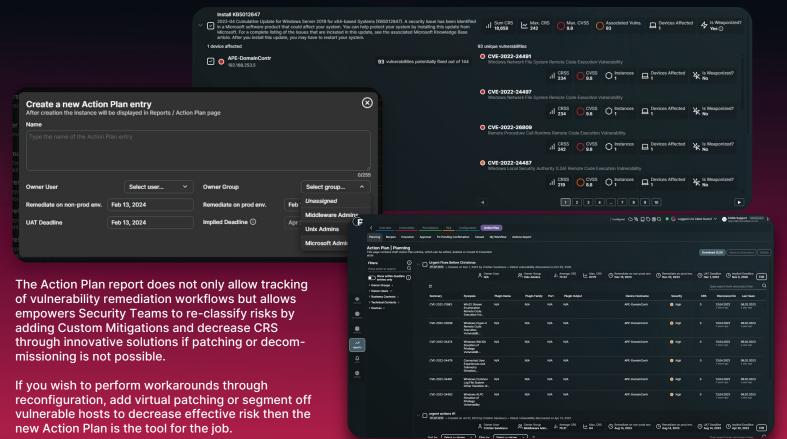


The Action Plan:

Our comprehensive Action Plan feature offers complete tracking of the remediation workflow from detection to fix confirmation.

Complete with remediation deadlines and alerts for breach of remediation schedule. Will allow assignment to remediation owners and approval of remediation actions so you can now efficiently manage each step of the process, ensuring timely resolution and minimizing potential risks.

This feature boosts cooperation between multiple teams as it allows assignment based on ownership, status update emails and complete audit tracking and approval requests for False Positive or Accept Risk actions.



It also tracks accepted risks and re-opens actions after the exception expired. It is also integrated with the scanning engine and can re-open actions where a scan has re-detected a previously closed vulnerability or even prevent closing of tickets where the scanner has not confirmed the fix through a new vulnerability scan.

	action e the action Urgent Fixes to	the Approval tab	\otimes
Reason			
(i) To edit the existing	ng mitigation options, go to C	client Settings in Settin	gs Menu
Mitigation options			
20%	Vorkaround ed IPS for known exploits		
75% Virtual Pa Added an I	tching PS for known exploits		
		Add a new mitigation	on option
Approval documents			
	Click to upload a new do	cument	
	Formats accepted: .pdf, .e	ml, .msg	
Accept Risk Deadline		Feb 13, 2024	

Summary:

Using the complete toolset offered by Coda Footprint empowers you to identify what needs to be addressed, prioritize and act toward remediation.

Then it offers complete tracking of actions and control of the remediation timeline with deadlines, alerts, and audit logs. True vulnerability lifecycle management in one complete solution.

Next steps:

Get in touch with your partner today to get the newest Collaborative Remediation capabilities enabled for your CODA Footprint environment!