

CR Vulnerability Disclosures

Reviewing the Security of the EKEN Smart Video Doorbell Camera Wireless with Chime Ringer and the Tuck Sharkpop Doorbell Camera Wireless

BY GLEN ROCKFORD, STEVE BLAIR AND DAVID DELLAROCCA FEBRUARY 29, 2004



EKEN Smart Video Doorbell Camera Wireless with Chime Ringer Vulnerability Disclosure

January 2024

Executive Summary

In January of 2024, Consumer Reports reviewed the security of the Eken Smart Video Doorbell Camera Wireless with Chime Ringer (Firmware: 2.8.1, App version: 2.8.2 (Eken Utilizes the Aiwit Application) The findings below were observed during testing:

1: The user's public facing IP is broadcast over the internet and network unencrypted. (Medium Risk)

2: Unauthenticated Access to JPEG via Server URL in [Vendor/Service] (High Risk)

3: The Users Local SSID is broadcast over the internet and network unencrypted. (Medium Risk)

4: Unauthorized Ownership of Video Doorbell (Aiwit Application) (High Risk)

Finding Number	Category	Risk	Exploitability	Impact	
1	1 Data Exposure		Medium	Medium	
2	2 Broken Access Control		High	High	
3	Data Exposure	Medium	Medium	Medium	
4	Unauthorized Ownership/Lack of Factory Reset Controls	High	High	High	



Detailed Findings

Finding 1: The user's public facing IP is broadcast over the internet and network unencrypted.

IP addresses are considered to be Personally Identifiable Information (PII) by multiple authorities including the CCPA (CCPA 1798.148 section V, 1A). Transmission of PII in cleartext does not meet best practices.

Once a user connects the device to their network, their public facing IP address is seen in the network traffic of the Wireless Security Camera in clear text (see screenshots below). (24.187.**).Testers External IP partially obscured in network capture image.



Finding 2: Unauthenticated Access to JPEG via Server URL in [Vendor/Service]

During network packet analysis, it was observed that a server is broadcasting a JPEG file without proper access controls; it is possible to intercept and download the JPEG file without the need for authentication. Within the captured packets, we identified the server's response containing the JPEG file.We were then able to extract the URL from the response, copy the extracted server URL from the log, open a web browser and paste the copied URL into the address bar, and the server fulfills the HTTP request without the need for authentication, allowing the unauthorized download of the JPEG file specified in the URL, By mimicking an IDOR (Insecure Direct Object Reference) Vulnerability. The server fulfills the HTTP request,



allowing the unauthorized download of the JPEG file specified in the URL. This poses a potential risk of unauthorized access to sensitive content. (See Screenshot Below)



Finding 3: The Users Local SSID is broadcast over the internet and network unencrypted.

During network packet analysis, it was observed that the local SSID (Service Set Identifier) is being broadcasted unencrypted and displayed in clear text during network communication. Exposure of the SSID in clear text poses a risk to user privacy and network security, increases the risk of unauthorized access to the network, potentially leading to unauthorized data access or manipulation. (See Screenshot Below)



	ken3filtered.pcap				– a x
Eil	<u>Edit View Go</u> Capture	Analyze Statistics Telephor	ıy <u>W</u> ireless <u>T</u> ools <u>H</u> elp		
	🗆 🔬 💿 💄 🗎 😫	🙆 🤇 🗢 🗢 혐 🖉	📃 📃 લ્લ્ 🖬		
	tcp.stream eq 39				×→ •
No.		Source	Destination	Protocol *	Length Info
-	2823 60.911441	192.168.137.148	47.243.224.28	TCP	🖉 Wireshark - Follow TCP Stream (tcp.stream eq 39) - eken3filtered.pcap - 🗆 🗙
	2852 61.165287	47.243.224.28	192.168.137.148	TCP	
	2853 61.178570	192.168.137.148	47.243.224.28	TCP	ime":"2024-01-06 05:20:35","video port":0,"web_domain":[{"host":"http://api.gdxp.com","ip":"4
	2854 61.178570	192.168.137.148	47.243.224.28	TCP	7.243.76.250"},{"host":"https://api.v2.gdxp.com","ip":"47.242.7.157"}],"what":131090}
	2889 61.467443	47.243.224.28	192.168.137.148	TCP	{"peer":"EKDB_0D39D9F6-215F-1860,"uid":"EKDB_0D39D9F6-215F-1860
	2890 61.467491	47.243.224.28	192.168.137.148	TCP	',"what":131093}
	2891 61.467512	47.243.224.28	192.168.137.148	TCP	{"what":131090, "uid":"EKDB_0D39D9F6-215F-1860 , "err_no":0}
	2893 61.486164	192.168.137.148	47.243.224.28	TCP	{"what":131093, "uid":"EKDB_0D39D9F6-215F-1860, "properties":{"PIR":2, "ri
	2894 61.486164	192.168.137.148	47.243.224.28	TCP	ng_volume":100, "firmware_ver":"2.1.8", "mcu_ver":"1.5.4", "wifi_ic"."Xm806", "wifi_dtim":6,
	2896 61.499084	192.168.137.148	47.243.224.28	TCP	"wifi_pm":2, "server_ip":"47.243.224.28", "rssi":-44, "ssid":" wifi_channel":0, "1
	2944 61.854561	47.243.224.28	192.168.137.148	TCP	ed_mode":0, "mac":"5c:1a:85:86:68:01", "device_faul
	2968 62.084365	192.168.137.148	47.243.224.28	TCP	{"what":131087, "ret":0, "uid":"EKDB_0D39D9F6-215F-1860, "mode":2, "state"
	3017 62.363796	47.243.224.28	192.168.137.148	TCP	:1, "info":{"chipdid":"62c05f002c0048200143c28a5076114f","battery_level":72, "reset_counnts":
	3023 62.405463	192.168.137.148	47.243.224.28	TCP	[0,0,0,0], "pir_counnts":[2,0,0,0], "pir_raw_counnts":[2,0,0,0], "led_day_night":0,"led_mode"
L	3068 62.695437	47.243.224.28	192.168.137.148	TCP	:0, "mcu_powerup_time":"2024-01-05 23:55:00[BT60PLUS][V:300.00(15.00)(0) 206.00(13.00)(0) (R:
					0 0 0 1) (wdr:0)][A: 22.00(43.00)(1024) 0.00(0.00)(0) volume:40 95][0 0 0 0 -1 0 2097151 -214
					7483648 34 27 0 0][ADC: 0 0(-83 -152 382 259 320 431) 0][BAT: 0 72 AXP0_0_18-55-10][NET: 5 5
					12 1000 12 1 39140072][BITRATE:0 0][NN:0 0 0 level:25][ip:192.168.137.148][205 81810176 0 130
					0][(tcp 47.251.7.44:9007)us,][1 0]", "ap_nat_type":0, "network_status":81810176, "heartbeat_n
					etwork_status":205, "wakeup_type":"PIR", "rssi":-46, "wakeup_count":2, "stream_speed":"000000
					00". "stream rate":0.000000. "pir count":0. "ring count":0. "adc value":0. "username":[]}}
					4 <mark>client</mark> pkts, 2 <mark>server</mark> pkts, 2 turns.
					Entire conversation (1933 bytes) Show data as ASCII Stream 39

Finding 4: Unauthorized Ownership of Video Doorbell (Aiwit Application)

During the course of testing the Eken video doorbell it was discovered that it is very easy for an unauthorized malicious actor to take full control of the video doorbell. Since this video doorbell does not have factory reset controls, an outside actor can exploit this to take ownership of the video doorbell. A malicious actor can put the doorbell into pairing mode simply by holding down the doorbell button for 8 seconds. The malicious user, who has simply downloaded the Aiwit app and has created their own account, can now scan the QR code generated by the app (The QR code is scanned simply by holding their mobile device screen up to the camera on the video doorbell). This QR code allows the video doorbell to connect to a different network (i.e. mobile hotspot set up by the malicious user). By scanning the QR code generated by the app for adding the video doorbell, they can successfully add the video doorbell to their account, gain control over a device that was originally associated with the homeowner's user account. The user who loses access to the doorbell will receive an email alerting them that ownership of their camera has changed. (See Screenshot Below). This is good, but until the owner of the video doorbell reads this email and can take the steps to reclaim it, the unauthorized malicious actor has full access to view and hear all activity picked up by the video doorbell.





Instructions to reset doorbell found here: <u>Eken Manual</u> Tester was unable to find any further instructions on factory resetting the doorbell. The only instructions found enable the device to enter pairing mode. (See Screenshots Below)





Possible Remediations

• Finding #1

- Don't store or transmit sensitive data unnecessarily.
- Encrypt all sensitive data at rest, ensuring up-to-date and strong industry standard algorithms, protocols and keys are in place. Use proper key management.
- Encrypt all data in transit with secure protocols and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS).
- Independent verification of the effectiveness of configuration and settings is ideal.

• Finding #2

- Encrypt all sensitive data in transit, ensuring up-to-date and strong industry standard algorithms, protocols and keys are in place. Use proper key management for the transmission of sensitive data from the devices, ensuring that the content remains confidential and protected from unauthorized access during transit.
- Implement stringent access controls on the server, requiring authentication. Such as; access token-based authentication mechanisms requiring valid tokens to control access to the server.

- Don't store or transmit sensitive data unnecessarily.
- Encrypt all sensitive data at rest, ensuring up-to-date and strong industry standard algorithms, protocols and keys are in place. Use proper key management.



- Encrypt all data in transit with secure protocols and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS).
- Independent verification of the effectiveness of configuration and settings is ideal.

- Secure Reset Mechanism: Develop and implement a secure factory reset mechanism that includes additional verification steps, making it resistant to unauthorized attempts.
- Device Identity Verification: Integrate device identity verification measures during the factory reset process, ensuring that only authorized users can initiate and complete the reset procedure.
- Multi-Factor Authentication (MFA): Enforce multi-factor authentication during the setup process to add an extra layer of security.
- Role-Based Access Control (RBAC): Implement RBAC to manage and restrict user access rights, ensuring that only authorized individuals have the necessary permissions to configure and control the video doorbell.

Tuck Sharkpop Doorbell Camera Wireless Vulnerability Disclosure

January 2024

Executive Summary

In January of 2024, Consumer Reports reviewed the security of the Tuck Sharkpop Doorbell Camera Wireless (Firmware: 2.8.1, App version: 2.8.2 (Tuck Utilizes the Aiwit Application) The findings below were observed during testing:

1: The user's public facing IP is broadcast over the internet and network unencrypted. (Medium Risk)

2: Unauthenticated Access to JPEG via Server URL in [Vendor/Service] (High Risk)3: The Users Local SSID is broadcast over the internet and network unencrypted.(Medium Risk)

4: Unauthorized Ownership of Video Doorbell (Aiwit Application) (High Risk)

Finding Number	Category	Risk	Exploitability	Impact	
1	1 Data Exposure		Medium	Medium	
2 Broken Access Control		High	High	High	
3	Data Exposure	Medium	Medium	Medium	
4	Unauthorized Ownership/Lack of Factory Reset Controls	High	High	High	



Detailed Findings

Finding 1: The user's public facing IP is broadcast over the internet and network unencrypted.

IP addresses are considered to be Personally Identifiable Information (PII) by multiple authorities including the CCPA (CCPA 1798.148 section V, 1A). Transmission of PII in cleartext does not meet best practices.

Once a user connects the device to their network, their public facing IP address is seen in the network traffic of the Wireless Security Camera in clear text (see screenshots below). (24.187.**).Testers External IP partially obscured in network capture image.



Finding 2: Unauthenticated Access to JPEG via Server URL in [Vendor/Service]

During network packet analysis, it was observed that a server is broadcasting a JPEG file without proper access controls; it is possible to intercept and download the JPEG file without the need for authentication. Within the captured packets, we identified the server's response containing the JPEG file.We were then able to extract the URL from the response, copy the extracted server URL from the log, open a web browser and paste the copied URL into the address bar, and the server fulfills the HTTP request without the need for authentication, allowing the unauthorized download of the JPEG file specified in the URL, By mimicking an



IDOR (Insecure Direct Object Reference) Vulnerability. The server fulfills the HTTP request, allowing the unauthorized download of the JPEG file specified in the URL. This poses a potential risk of unauthorized access to sensitive content. (See Screenshot Below)

2 1	tuckfiltered.pcap							- 🗆 ×
Eile	e <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> aptu	re <u>A</u> nalyze <u>S</u> tatistics Telephor	ny <u>W</u> ireless <u>T</u> ools <u>H</u> elp					
	🔲 🔬 🎯 💄 🗎 🖄	। 🙆 🤏 🗢 🗢 🖉 🖉 💆	📃 📃 ବ୍ର୍ବ୍ 🖬					
	tcp.stream eq 6							×= +
No.			Destination		enath Info			
+	147 19.510655	192.168.137.213	47.243.228.110	HTTP		tion?udid=EKDB 371CE59E-		event=PIR&endpoint=http:/
+	152 19.794964	47.243.228.110	192.168.137.213	HTTP	341 HTTP/1.1 200 OK (
E	139 19.220724	192.168.137.213	47.243.228.110	TCP	74 45734 → 58720 [SYN] Seq=0 Win=29200 Len=0	MSS=1460 SACK PERM TSval=	4294937531 TSecr=0 WS=8
	145 19.490683	47.243.228.110	192.168.137.213	TCP	74 58720 → 45734 [SYN	, ACK] Seq=0 Ack=1 Win=6	5160 Len=0 MSS=1460 SACK	PERM TSval=1657538937 TSecr=
Т	146 19.510655	192.168.137.213	47.243.228.110	TCP			Len=0 TSval=4294937560 TS	ecr=1657538937
	151 19.794879	47.243.228.110	192.168.137.2:	Wireshark - Follow TCP	Stream (tcp.stream eq 6) · tuckfiltered.	pcap		– 🗆 ×
	153 19.817176	192.168.137.213	47.243.228.110					
	154 19.818619	192.168.137.213			fication?udid=EKDB_371CE			t=http://oss-us-west-1.al
	171 20.101132	47.243.228.110				file_name=/20240104/1505	5/150517_262836907_EKDB_37	1CE59E-935A
L	172 20.121935	192.168.137.213		FFEF8ACDB.jpg				
				Host: 47.243.2	28.110			
				HTTP/1.1 200 0				
					Jan 2024 20:05:19 GMT			
				Content-Length		_		
				Content-Type: *	text/plain; charset=utf-	8		
				{"resultCode":	0,"msg":"https://usw-aiv		t-1.aliyuncs.com//20240104	/1505/150517_262836907_EK
				DB_371CE59E-		.jpg"}		
				<mark>client</mark> pkt, 1 <mark>server</mark> pkt, 1 turi				
				Entire conversation (547	' bvtes) 👻	Shor ASCII	•	Stream 6
				Entitle conversation (547	bytes)	Silo Asci		Siteani o 👻
				ind:				Find Next
						Filter Out This Str	eam Print Save as	Back Close Help
						The out mask	Can I Int Dave com	close help
•								•
		tes on wire (2704 bits					51 be af 2d 08 00 45 00	•• <x•• -="" e<="" q="" s="" td=""></x••>
							ac 43 c0 a8 89 d5 2f f3	D.@@ C···/
		Version 4, Src: 192.1					a5 35 21 bc 16 33 80 18	
			:: 45734, Dst Port:	58720, Seq: 1		0e 42 9d 39 00 00 01 01	08 0a ff ff 8b d8 62 cc	
2	Hypertext Transfer	r Protocol			0040			yGET /f ile_noti
								fication ?udid=EK
								DB_371CE 59E-935A
								//oss-us -west-1.
					0060			aliyuncs .com&buc

Finding 3: The Users Local SSID is broadcast over the internet and network unencrypted.

During network packet analysis, it was observed that the local SSID (Service Set Identifier) is being broadcasted unencrypted and displayed in clear text during network communication. Exposure of the SSID in clear text poses a risk to user privacy and network security, increases the risk of unauthorized access to the network, potentially leading to unauthorized data access or manipulation. (See Screenshot Below)



tream eq 33			Wireshark - Follow TCP Stream (tcp.stream eq 33) - tuckfiltered.pcap	
Time	Source	Destination	{"what":131073, "uid":"EKDB_371CE59E-935A-0A47-67AC-DA7FFEF8ACDB", "state":1, "mode":2, "cate	gory":"unknow",
1890 52.839514	192.168.137.213	47.243.224.28	akeup_type":"PIR", "vendor":1, "version":"v1", "k":"0bd10fea7ced5d1f993b1a904a6395991"}	
897 53.082455	47.243.224.28	192.168.137.2		
1898 53.097516	192.168.137.213	47.243.224.28		ost":"https://a
899 53.097835	192.168.137.213	47.243.224.28	v2.gdxp.com","ip":"47.242.7.157"}],"what":131090}	
909 53.387967	47.243.224.28	192.168.137.2	{"peer":"EKDB_371CE59E-935A","uid","uid":"EKDB_371CE59E-935A","uid"	","what"
910 53.388020	47.243.224.28	192.168.137.2	1093}	
911 53.388037	47.243.224.28	192.168.137.2	{"what":131090, "uid":"EKDB 371CE59E-935A ", "err no":0}	
912 53.404622	192.168.137.213	47.243.224.28		
913 53.404763	192.168.137.213	47.243.224.28	irmware ver":"2.1.8", "mcu ver":"1.5.4", "wifi ic":"XR806", "wifi dtim":6, "wifi pm":2, "serve	er ip":"47.243.
914 53.427009	192.168.137.213	47.243.224.28	.28", "rssi":-44, ssid":" ", "wifi channel":0, "led mode":0, "mac":"9c:53:51:be:af:2d	', "device faul
935 53.770252	47.243.224.28	192.168.137.2		
946 54.035539	192.168.137.213	47.243.224.28	{"what":131087, "ret":0, "uid":"EKDB 371CE59E-935A ", "mode":2, "state"	1, "info":{"ch
961 54,306389	47,243,224,28	192,168,137,2	id":"62c05f004c00482001454581484e13cf","battery level":356, "reset counnts":[0,0,0,0], "pir co	ounnts":[2.0.0.
969 54,426456	192.168.137.213	47.243.224.28		
975 54.716399	47.243.224.28	192.168.137.2		
112 69.746799	47.243.224.28		0 -1 0 2097151 -2147483648 36 29 0 0][ADC: 0 0(-77 -154 462 238 294 431) 0][BAT: 1 100 AXP0 0	
113 69.784175	192.168.137.213		0 146 12 0 1 0 42301100][BITRATE:0 0][NN:0 0 0 level:25][ip:192.168.137.213][204 81810180 0 1	
401 75.218049	192.168.137.213	47.243.224.28		
404 75,503011	47,243,224,28	192.168.137.2		
405 75.503061	47.243.224.28	192.168.137.2		Stream
406 75.540418	192.168.137.213	47.243.224.28		
407 75.811644	47.243.224.28	192.168.137.2		Fin
408 75.826867	192,168,137,213	47.243.224.28		Close
ernet II, Src:	tes on wire (3232 bit 9c:53:51:be:af:2d (9c Version 4, Src: 192.1	::53:51:be:af:2d)	, Dst: 96:e2:3c:78:98:17 (96:e2:1 0010	SQ - E @@C< / "1 8
nsmission Contr a (338 bytes)	ol Protocol, Src Port	:: 48322, Dst Por	0040	what ":131093 id": "EKDB_37
			0070	

Finding 4: Unauthorized Ownership of Video Doorbell (Aiwit Application)

During the course of testing the Tuck video doorbell it was discovered that it is very easy for an unauthorized malicious actor to take full control of the video doorbell. Since this video doorbell does not have factory reset controls, an outside actor can exploit this to take ownership of the video doorbell. A malicious actor can put the doorbell into pairing mode simply by holding down the doorbell button for 8 seconds. The malicious user, who has simply downloaded the Aiwit app and has created their own account, can now scan the QR code generated by the app (The QR code is scanned simply by holding their mobile device screen up to the camera on the video doorbell). This QR code allows the video doorbell to connect to a different network (i.e. mobile hotspot set up by the malicious user). By scanning the QR code generated by the app for adding the video doorbell, they can successfully add the video doorbell to their account, gain control over a device that was originally associated with the homeowner's user account. The user who loses access to the doorbell will receive an email alerting them that ownership of their camera has changed. (See Screenshot Below). This is good, but until the owner of the video doorbell reads this email and can take the steps to reclaim it, the unauthorized malicious actor has full access to view and hear all activity picked up by the video doorbell.





Possible Remediations

- Don't store or transmit sensitive data unnecessarily.
- Encrypt all sensitive data at rest, ensuring up-to-date and strong industry standard algorithms, protocols and keys are in place. Use proper key management.
- Encrypt all data in transit with secure protocols and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS).
- Independent verification of the effectiveness of configuration and settings is ideal.



- Finding #2
 - Encrypt all sensitive data in transit, ensuring up-to-date and strong industry standard algorithms, protocols and keys are in place. Use proper key management for the transmission of sensitive data from the devices, ensuring that the content remains confidential and protected from unauthorized access during transit.
 - Implement stringent access controls on the server, requiring authentication. Such as; access token-based authentication mechanisms requiring valid tokens to control access to the server.
- Finding #3
 - Don't store or transmit sensitive data unnecessarily.
 - Encrypt all sensitive data at rest, ensuring up-to-date and strong industry standard algorithms, protocols and keys are in place. Use proper key management.
 - Encrypt all data in transit with secure protocols and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS).
 - Independent verification of the effectiveness of configuration and settings is ideal.

- Secure Reset Mechanism: Develop and implement a secure factory reset mechanism that includes additional verification steps, making it resistant to unauthorized attempts.
- Device Identity Verification: Integrate device identity verification measures during the factory reset process, ensuring that only authorized users can initiate and complete the reset procedure.
- Multi-Factor Authentication (MFA): Enforce multi-factor authentication during the setup process to add an extra layer of security.
- Role-Based Access Control (RBAC): Implement RBAC to manage and restrict user access rights, ensuring that only authorized individuals have the necessary permissions to configure and control the video doorbell.



EXTERNAL AUDIENCE PROTOCOL

External Audience Protocol (EAP) - Video Doorbells Privacy Testing

©2024 Consumer Reports, Inc. This document is the property of Consumer Reports and is intended for the recipient's internal use only. You may not republish this document or provide copies to third parties or authorize anyone else to do so without Consumer Reports' prior written consent. You may not use or authorize any third party to use Consumer Reports' names, ratings or trademarks (i) in any form of advertising, marketing or promotion; (ii) in any manner that may be construed as an endorsement by Consumer Reports; or (iii) in any manner inconsistent with CR's <u>No-Commercial Use Polic</u>y without Consumer Reports' prior written consent.

This document's contents may not be used in connection with any legal proceedings (including but not limited to litigation involving warranties, marketing claims, product liability, market share, injury or property), regulatory standard setting, administrative investigations or enforcement proceedings, or in connection with any other type of proceedings to which Consumer Reports is not a party. This document is otherwise subject to the terms of Consumer Reports' <u>User Agreement</u>. Learn more at *CR.org*.

Purpose of this document:

This document is generated by the testing team to describe what tests are done in our evaluation of data privacy and security of Video Doorbells. Specifically, it refers to the relevant criteria and indicators from the Digital Standard that apply to this testing. It also provides an overview of our testing methodologies.

Who was this created for?

The primary audience for this document is Video Doorbell manufacturers, who are typically interested in understanding what our tests are looking for and what our ratings are based on.

Introduction

Video Doorbells are increasing in popularity due to dropping prices and more consumer interest. They provide users with access to video and audio footage, live or recorded, over the internet, which presents the possibility for this data to be accessed, stored, shared, bought, sold, and stolen. Therefore, the security and privacy of these Video Doorbell Cameras is a primary concern for consumers and Consumer Reports. Not only do we need to test the performance of Video Doorbells (e.g. clarity, convenience) but also make sure the Video Doorbell Camera is protecting the owner, not monitoring them.

Test Description

Products are tested in accordance with the following criteria/indicators of the Digital Standard (<u>https://www.thedigitalstandard.org/</u>).

Privacy

- 1. Data Control I can see and control everything the company knows about me.
 - a. Users can control the collection of their information.
 - b. Users can delete their information.
 - c. Users can control how their information is used to target advertising.
 - d. Users can obtain a copy of their information.
 - e. Clear explanations of how users can control their data.
 - f. Privacy controls exist and are effective.
- 2. Data Share Data sharing is reasonably scoped and transparent.

- a. The company only shares information with third parties as is reasonably necessary to deliver service to consumers.
- b. The company clearly discloses what user information it shares with whom.
- c. The company clearly discloses the types of third parties with which it shares user information.
- d. The company clearly discloses the names of third parties with which it shares user information.
- e. The company clearly discloses whether it shares user information with government or legal authorities.
- f. Third-party domains contacted by the product are named in the privacy policy.
- 3. Data Use Data usage is consistent with the context of the relationship with the user and is transparent.
 - a. The company puts limits on the use of my data that is consistent with the purpose for which the data is collected.
 - b. The company explicitly discloses every way in which it uses my data.
- 4. Data Retention and Deletion I know how long the company keeps my information.
 - a. All user information is deleted after users terminate their accounts or remove service from a device.
 - b. Disclosure of timeframe in which user information is deleted after users terminate their account.
 - c. Disclosure of how long each type of user information is retained.
- 5. Data Collection I know what user information this company is collecting and when.
 - a. Disclosure of the type of user information collected.
 - b. Disclosure of how user information is collected.
 - c. The device gives clear indication (e.g., lit LED) when cameras and microphones are active.
- 6. Minimal Data Collection The only information the company requests from me is what's needed to make the product or service work correctly.
 - a. The user information collected is only that which is directly relevant and necessary for the service.
 - b. The product still works when all permissions not relevant to the product's functionality are declined.
- 7. Privacy by Default The default settings in this product prioritize my privacy; to give up privacy, I actually need to change the settings.
 - a. Targeted advertising is off by default.
 - b. User interface settings that are optimal for privacy are set by default.
- 8. Data benefits Every piece of data I share brings me a benefit; it doesn't just help the company.
 - a. The company clearly discloses its purpose for collecting each type of user information.
- 9. Data benefits Every piece of data I share brings me a benefit; it doesn't just help the company.
 - a. The company clearly discloses its purpose for collecting each type of user information.

- 10. Terms of Service and Privacy Policy documents I can easily find, read, and understand the privacy policy and/or terms of service.
 - a. The company clearly discloses which Terms of Service (ToS) apply to the product/service in question.
 - b. The ToS are easy to find.
 - c. The company clearly discloses which Privacy Policy (PP) applies to the product/service in question.
 - d. The PP is easy to find.
- 11. ToS & Privacy Policy change notification The company provides clear notification when it changes its privacy policy and/or terms of service.
 - a. Commitment to notify users about changes to the terms of service
 - b. Maintains a public archive or change log of the terms of service
 - c. Commitment to notify users about change to the privacy policy
 - d. Maintains a public archive or change log of the privacy policy

Security

- 12. Encryption Information I provide is encrypted so that it can't be easily read or used by attackers.
 - a. All transmission of user communications is encrypted by default.
 - b. All transmission of user communications is encrypted by a secure algorithm.
 - c. Users can secure their content using end-to-end encryption.
 - d. End-to-end encryption is enabled by default.
- 13. Known Exploit Resistance The product is protected from known software vulnerabilities that present danger from attackers.
 - a. The software is secure against known bugs and types of attacks.
 - b. All known CVE or CWE should be fixed.
- 14. Authentication A product has an authentication system that corresponds to the sensitivity of the user data it manages. And a product that has an authentication system resists attempts to break it.
 - a. If a product supports user accounts, it has an authentication system for accessing those accounts.
 - b. If the product uses a password/passphrase for authentication, it allows all reasonable characters as input.
 - c. If the product uses a password/passphrase for authentication, it requires that passwords are at least 8 characters long.
 - d. If the product uses a password/passphrase for authentication, the password/passphrase may be at least 20 characters long.
 - e. If the product uses a password/passphrase for authentication, it requires that passwords are reasonably complex.
 - f. If the product uses a password/passphrase for authentication, it is compatible with popular password managers.
 - g. If a product is packaged with an account with default credentials, those credentials are unique to the instance of the product
 - h. If a product has an authentication system, the user must authenticate each time they want to use the product

- i. If a product has an authentication system, it requires at least two pieces of information to authenticate users
- j. For products that handle sufficiently sensitive data, users can choose to use multi-factor authentication.
- k. For products that handle sufficiently sensitive data, users can choose to use multi-factor authentication whenever the product is activated, or when a device is unrecognized.
- I. The product allows users to be notified via an out-of-band medium when account security settings are changed.
- m. To change a password/passphrase/pin, a user must enter the previous password/passphrase/pin, or have access to a secondary system that is used to reset it.
- n. The product notifies users when account security settings have changed.
- o. If the product has an authentication system, it also has a system to prevent brute-force/dictionary attacks
- 15. Security Oversight The company is a responsible caretaker of my data.
 - a. The company has systems in place to limit and monitor employee access to user information.
 - b. The company has an internal security team that conducts security audits on the company's products and services.
 - c. The company commissions third-party security audits on its products and services.
- 16. Security Over Time The product is kept protected with software updates for a clearly defined and communicated period of time (i.e., the product life cycle).
 - a. The product life cycle is communicated to the potential owner before purchase.
 - b. Software updates are authenticated.
 - c. Automatic software updates
 - d. Notification of software updates
 - e. Ease of installation of software updates
 - f. The software can be kept up-to-date for security issues.
- 17. Vulnerability Disclosure Program The company is willing and able to address reports of vulnerabilities.
 - a. The company has a mechanism (ex: a bug bounty program) through which security researchers can submit vulnerabilities they discover.
 - b. The company discloses the timeframe in which it will review reports of vulnerabilities.
 - c. The company commits not to pursue legal action against security researchers.

Test Methodology

CR Privacy & Security Testing consists of three primary methodologies outlined below.

- 1. UI/UX Evaluation
 - Test the Password creation rules to determine the level of complexity required.
 - Test and look for requirements for additional user authentication options (Bio, MFA, PIN, and etc.)
 - Validate Firmware update options offered.
 - Validate Software update options offered.
 - CVE database known exploits lookup.
 - Review data control options in UI/UX.
- 2. Technical Test
 - Security features (Set up the device and note the privacy/security settings and features available to the user, such as cert pinning, root detection, backup option, stack protection, etc.)
 - Perform an extensive Brute-force dictionary attack.
 - Continuous network traffic capture, processing and analysis to validate that all data is encrypted in transmission.
 - Data encryption at rest (Local file system inspection). Validate that all data created or information stored locally on the host device is encrypted.
 - Perform Vulnerability scanner testing (i.e., light penetration testing).
 - Confirm if CVE database known exploits are fixed.
 - Detect third-party tracker's SDKs.
 - Analyze network traffic endpoints.
- 3. Document Review
 - CR reviews privacy policies, terms of service, EULA and other public, legally binding, documentation to determine what practices a company commits to in writing.