MONITORING & INCIDENT RESPONSE

Introduction

By 2025, forecasts predict that there will be more than 450 million connected vehicles on the road. The increasing capabilities offered by connected computer systems enable a wide array of digital services and features. Modern vehicles can have up to 100 embedded systems, which makes the vehicle a network on wheels. The technological evolution, together with the expanding attack surface (remote interfaces), increases the number of vulnerabilities and techniques that are likely to be used by attackers to compromise a vehicle or the entire fleet.

🛦 Challenges

Every component in a modern vehicle has at least dozens of opensource libraries, therefore, has thousands of known vulnerabilities and exploits.

Automotive companies are now required to implement vulnerability management processes to comply with the new regulations. The processes include monitoring and mitigation of cybersecurity vulnerabilities, not only for themselves but also for partners, third parties, and service providers during the entire supply chain and vehicle lifecycle (cross models, platforms, and versions). The number of vulnerabilities and attacks increases every day. Therefore, manufacturers and Tier 1 suppliers must always have clear monitoring and visibility in order to make critical decisions in real time that prevents and minimizes the damage to the vehicle or driver.



! The Solution

CYMOTIVE cyber automotive specialists and forensics team are researching how attackers and cyber criminals behave. The team detects and responds to cyberattacks in connected vehicles, services, and fleets by defining new cyber processes, building risk model methodologies and mitigation plans for its customers. The processes can be customized to the regulation standards in the relevant countries. Our Attack Research Lab (ARL) possess proven end-to-end incident detection and response capabilities. By elevating our vast knowledge of the attacker's perspective, we have established evidence-based detection mechanisms that use correlation rules, machine learning, and threat intelligence capabilities.



Vehicle Logs Analysis

Our CarAlert system maps and manages vulnerabilities in the fleet level, including software packages and ECUs, measuring overall security and business implications to reach optimal decision making. In order to detect, assess, and prioritize un-mitigated vulnerabilities, we collect data from

Image: Non-State State Construction Con					-	_							
No. Open Variantia Open Variantia <th>Cereral Information Partitione</th> <th>Assets Maluh I</th> <th>tal Dates</th> <th>stepad Survio</th> <th>9 Q</th> <th>*</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>Cita Ho</th>	Cereral Information Partitione	Assets Maluh I	tal Dates	stepad Survio	9 Q	*							Cita Ho
Allocation Allocation Status Status <td< th=""><th>Group</th><th>10</th><th>Severity</th><th>Equip</th><th>5009</th><th>CV55 THEBA</th><th>Carlet Scre</th><th>CanAlwrit Chtis Wector</th><th>Public Over</th><th>todated At</th><th>Description</th><th>her.</th><th></th></td<>	Group	10	Severity	Equip	5009	CV55 THEBA	Carlet Scre	CanAlwrit Chtis Wector	Public Over	todated At	Description	her.	
MANDERING MANDERING <t< td=""><td> debut;petition/400; </td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	 debut;petition/400; 												
Allowers, C. Automatics, State (1994) State (1994) Nature State, State (1994) C Automatics, State (1994) State (1994) Nature State, Sta	> Issesterate \$18(1)												
O Aukonski, O Aukonski, Statu III.0000 Natura III.0000 Natura III.0000 0 Aukonski, Statu III.0000 Statu III.0000 Statu III.0000 Natura III.0000 0 Aukonski, Statu III.0000 Statu III.0000 Natura III.0000 Natura III.0000 0 Aukonski, Statu III.0000 Statu III.0000 Natura III.0000 Natura III.0000 0 Aukonski, Statu III.0000 Statu III.0000 Statu III.0000 Natura III.0000 0 Aukonski, Statu III.0000 Statu III.0000 Statu III.0000 Statu III.0000 Statu III.0000 0 Aukonski, Statu III.0000 Statu III.0000 Statu III.0000 Statu III.0000 Statu III.0000 0 Aukonski, Statu III.0000 Statu III.0000 Statu III.0000 Statu III.0000 Statu III.0000 0 Aukonski, Statu III.00000 Statu III.00000 Statu III.00000 Statu III.00000 Statu III.000000 0 Aukonski, Statu III.000000 Statu III.000000 Statu III.000000 Statu III.0000000 Statu III.000000000000 Statu III	~ operar(1020(72)												
O Aukoman. O Aukoman. Aukoman.<		05,225,0736	MEDIUM	NA	0	ANNALHIBRY.	0	ANNOLINA SUC.	10/00/0014 12:29:00 PM	8:04:0000, 5:07:00 PM	The OpenSSL 05A s-		
O AND/ONLY O AND/ONLY Name <		0522523	MOUN	NA		AUNICHIMAL	0	WHENCHPRNUNSUC.	10/90/2018 12/2000 PM	8-24/2020 5-31/00 PM	The OperSti, DSA p		
0 Aukontosis. 0 Aukontosis. 0 Aukontosis. 0 <t< td=""><td></td><td>255,825,622</td><td>NOW</td><td>NA</td><td></td><td>ANACHIROL.</td><td>0</td><td>ANICHRINUNSUC.</td><td>416/2018 62900 PM</td><td>10/9/2018 12/00/00 AM</td><td>The OpenSSLRSA K.</td><td></td><td></td></t<>		255,825,622	NOW	NA		ANACHIROL.	0	ANICHRINUNSUC.	416/2018 62900 PM	10/9/2018 12/00/00 AM	The OpenSSLRSA K.		
O AudoRosis O AudoRosis O ISIDI INIM I ISIDI INIM I Ionamatoria 0 AudoRosis 0 AudoRosis I Ionamatoria I Ionamatoria I Ionamatoria 0 AudoRosis 0 AudoRosis I Ionamatoria I Ionamatoria I Ionamatoria 0 AudoRosis 0 AudoRosis I Ionamatoria I Ionamatoria I Ionamatoria 0 AudoRosis 0 AudoRosis I Ionamatoria I Ionamatoria I Ionamatoria I Ionamatoria 0 AudoRosis 0 I Ionamatoria I Ionamatoria I Ionamatoria I Ionamatoria I Ionamatoria 0 AudoRosis <		05278.507	MOUN	65785	•	ALCOHOLD.	•	INVICERIUMSUCK-	1115/2018 92900 PM	818/3020 4/88/00 PM	Simularesia Multi-		
0 Aukohmish 0 Aukohmish 0 Aukohmish 0 <td></td> <td>05425450</td> <td>NEDUM</td> <td>1010</td> <td>•</td> <td>AUXONPRUM.</td> <td>•</td> <td>AUXINELUNSUON.</td> <td>1115/2018 92900 PM</td> <td>815/2020 4/5000 PM</td> <td>Smutaneous Muti</td> <td></td> <td></td>		05425450	NEDUM	1010	•	AUXONPRUM.	•	AUXINELUNSUON.	1115/2018 92900 PM	815/2020 4/5000 PM	Smutaneous Muti		
0 ALACHARAN 0 ALACHARAN DERIS MANA		05.275.150	MOUN	NA		AUGACHINGUN-		AURCHIMUM SUCH-	\$1000FR \$1500 PM	10/20/0020, 10/15/00 PM	Normaly in OpenSS-		
0 Aukolimuk 0 Aukolimuk 2021 10241 1021 10241 Faugurese. 0 Aukolimuk 0 1021 1024 1021 10241 1021 1024 Faugurese. 0 Aukolimuk 0 400401000406. 1021 10240 1021 1024 <t< td=""><td></td><td>05479-002</td><td>(LOW)</td><td>NA</td><td>33</td><td>AUXCORUM.</td><td>33</td><td>AURCHMUNISUCNI.</td><td>190 2018, \$1500 PM</td><td>13/25/2020, 13/15/00 PM</td><td>Oper33, ras interna.</td><td></td><td></td></t<>		05479-002	(LOW)	NA	33	AUXCORUM.	33	AURCHMUNISUCNI.	190 2018, \$1500 PM	13/25/2020, 13/15/00 PM	Oper33, ras interna.		
0 Aukomini, 0 Aukominication, 10201 (1000) Teatmann, 10201 (1000) Teatmann, 1020 (1000) 0 Aukomini, 0 Aukominication, 10201 (1000) SIGE (1000) SIGE (1000) SIGE (1000) 0 Aukominication, 10201 (1000) SIGE (1000) SIGE (1000) SIGE (1000) SIGE (1000) 0 Aukominication, 1020 (1000) SIGE (1000) SIGE (1000) SIGE (1000) SIGE (1000) 0 Aukominication, 1020 (1000) SIGE (1000) SIGE (1000) SIGE (1000) SIGE (1000)		0.0.2219.1538	NOW	NA	69	ANNACHTRAL.	63	ANNOLANUNSUO.	2/07/2019 11/29/00 PM	109/0021, 31500 PM	Far application enc.		
8 AnkOntoxica, 1992 Statistica Statis Statistica <td></td> <td>0.8.2718-1988</td> <td>LECUN</td> <td>NA</td> <td></td> <td>Anacemey.</td> <td>0</td> <td>ANSCHMINUNSUO.</td> <td>2/07/2018 11/29/00 PM</td> <td>1/20/2021, \$1500 PM</td> <td>Far application and</td> <td></td> <td></td>		0.8.2718-1988	LECUN	NA		Anacemey.	0	ANSCHMINUNSUO.	2/07/2018 11/29/00 PM	1/20/2021, \$1500 PM	Far application and		
0 Anacherous 0 Anacherous 0.212211303/M 0.52211303/M 0.5221130/M 0.5221130/M <td></td> <td>05329-190</td> <td>(10%)</td> <td>NA</td> <td>37</td> <td>AUNIACHIPRIN-</td> <td>(57)</td> <td>ANNONRAUMSUICE.</td> <td>\$10:2018 \$1500 PM</td> <td>15/20/0020, 10/15/00 PM</td> <td>instations share a</td> <td></td> <td></td>		05329-190	(10%)	NA	37	AUNIACHIPRIN-	(57)	ANNONRAUMSUICE.	\$10:2018 \$1500 PM	15/20/0020, 10/15/00 PM	instations share a		
ANALONKY.		052212360	623	NA	•	Annacommu.		ANNOUNNINGUES.	2/16/2021, 5/15/00 PM	620217190074	Crists 5/7, Coher-	Denial Of Service	
C ACIECTRICO. C ACIECTRICANDOCIN. EVIDE ADDOLES 111021(1380384 COPINIPAREL.		05225-2391	MEDION	NA	- 53	AUXACINIPRIN-	53	REVERSION REVENUES	2/16/2021, 51500 PM	\$25(2021, 71200 PM	The OpenSSL public	Denial OF Service	
C AURCHINGE AURCHINGENCE \$1/18(40003M \$11001(10003M DHFMMMANE).	 Inux kernel 44,152 (526) 												
		01/05/02	NA	NA	0	AVEACEPRINE.	0	INCICL/RNUNSCON.	8/1/1997, 40000 AM	5/11/2017; 12900.MM	OUP internation to		
B ANNAL MANUL B ANNAL MANUNAL STUTME \$0000 MM STUDIES TO BE AND THE UP OF THE AND THE		045.1895.0656		NA	•	ANNOURAU.	•	INNICURNUNSCOL.	1/1/1998 \$0000.AM	311/2017; 12900.MM	The up of RPC intert.		
Annacuments Annacumen	 Inus serie 44.12 (20); W1.4991.000; Base 			NA NA NA NA	53 (5) (5) (5) (5)	Annenfinger Annenfinger Annenfinger Annenfinger		ANICHRINISCUC. ANICOMINATION MURCHRINISCOL AURCHRINISCOL MURCHRINISCOL	810201831500 PM 216200151500 PM 216200151500 PM 216200151500 PM 2177998 80000 AM	1920-0202 121500 PM 6-02020, 121500 PM 5-02420, 12100 PM 5-02420, 12100 PM 5-014201, 12000 AM	In studios when Gris to BVP, Carke The OpenSS, public ICMP internation is The upper RPC inte	8 6 8	ь. с (она сталов) к. (она сталов) к. (она сталов) к.
	upotella Marca 💷												
	Mach Vester (NV)	Atlack Complexity (Ad	5	Prinleges Requir	ed (PR)	User Interaction (an	Doope (E)					
(1991) User Menualise (U) Doree (D)													
4(P0) [34:Heydels (3)] [36:es (5) [36:es] [36:es] [36:	mpact Metrics (1)												
474() Der Mander 50) Bere 8 Aus Dariel	Confidentiality (C)	Hagity (I)		Availability (A)									
4/% Use House (0) Soon (0) Inco (Consert													

CarAlert Vulnerability Dashboard

several sources, such as the CarAlert system, IDS, threat intelligence, penetration testing, and others. The unique processes, together with the analysts' knowledge-base and unique experience, give us the ability to analyze the E2E perspective needed to mitigate vulnerabilities and to respond to cyber incidents.

