# Missing Session Revocation on Logout in ash_authentication_phoenix

Low **zachdaniel** published **GHSA-f7gq-h8jv-h3cq** on Jun 17, 2025

**Package**

**ash_authentication_phoenix** (Erlang)

**Affected versions**

<= 2.9.0

**Patched versions**

>= 2.10.0

**Description**

## Impact

Session tokens remain valid on the server after user logout, creating a security gap where:

- Compromised tokens (via XSS, network interception, or device theft) continue to work even after the user logs out
  - The sessions stored in the database still expire, limiting the duration during which this could be exploited
- Users cannot fully invalidate their sessions when logging out from shared or potentially compromised devices
  - by default, changing one's password *does* invalidate all other sessions, so changing your password as a security measure would have been effective
- May cause compliance issues with security frameworks requiring complete session

## Patches

Upgrade to version 2.10.0. After upgrading, users must update their AuthController implementation to use the new `clear_session/2` function with their OTP app name. You will be prompted to do so with a compile-time error.

If you do not have the setting `require_token_presence_for_authentication?` set to `true` in the `tokens` section, you will see a separate error:

```
** (Spark.Error.DslError) authentication -> session_identifier:
Must set `authentication.session_identifier` to either `:jti` or `:unsafe`.

...
```

In order to revoke sessions on log out when not storing tokens directly in the session, we must have some unique identifier with which to do so. You should prefer to enable `require_token_presence_for_authentication?` if possible, instead of setting this to `:jti`. Note that whatever you do here, if you did not previously have `require_token_presence_for_authentication?` set to `true`, setting it to `true` *or* setting `authentication.session_identifier` to `:jti` will log out all of your currently authenticated users.

## Workarounds

You can manually revoke tokens in your `logout/2` handler in your auth controller.

**Severity**

Low 2.3 / 10

**CVSS v4 base metrics**

| | |
|---|---|
| **Exploitability Metrics** | |
| Attack Vector | Network |
| Attack Complexity | Low |
| Attack Requirements | Present |
| Privileges Required | None |
| User interaction | Passive |
| **Vulnerable System Impact Metrics** | |
| Confidentiality | Low |
| Integrity | Low |
| Availability | None |
| **Subsequent System Impact Metrics** | |
| Confidentiality | None |
| Integrity | None |
| Availability | None |

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

**CVE ID**

CVE-2025-4754

### Weaknesses

▶ CWE-613

### Credits

| | |
|---|---|
| **jimsynz** | Remediation reviewer |
| **zachdaniel** | Remediation developer |
| **mbuhot** | Analyst |
| **maennchen** | Analyst |