

wildfly-security / wildfly-elytron Public

<> Code **Pull requests** 34 Actions Projects Wiki Security and quality 1

[ELY-2887] Add a nonce to OIDC requests for CVE-2024-12369 #2253

Closed rsearls wants to merge 1 commit into wildfly-security:2.x from rsearls:JBEAP-28701-OIDC-Auth-Code

Conversation 108 Commits 1 Checks 9 Files changed 13

rsearls commented on Feb 11, 2025 • edited Contributor

<https://nvd.nist.gov/vuln/detail/CVE-2024-12369>
<https://issues.redhat.com/browse/JBEAP-28701>

rsearls requested review from **fjuma** and **skyllarr** as code owners last year

fjuma requested changes on Feb 11, 2025

View reviewed changes

http/oidc/src/main/java/org/wildfly/security/http/oidc/Oidc.java Show resolved

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java Outdated Show resolved

```

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java Outdated
457 | 460 |           return challenge(HttpStatus.SC_FORBIDDEN, AuthenticationError
458 | 461 |         }
    | 462 | +
    | 463 | +           String stateCookieValue = getCookieValue(deployment.getStateCool

```

fjuma on Feb 11, 2025 Contributor

A separate cookie should be used for nonce purposes.



rsearls on Feb 17, 2025

Contributor Author

done

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java

Outdated

```

463 + String stateCookieValue = getCookieValue(deployment.getStateCookieName());
464 + String nonceValue = token.getClaimValueAsString(NONCE);
465 + if (nonceValue == null || !nonceValue.equals(String.valueOf(stateCookieValue)))
466 +     log.error("Invalid nonce");

```



fjuma on Feb 11, 2025

Contributor

I think it would be better to validate the nonce in the `TokenValidator#parseAndVerifyToken` method here:

<https://github.com/wildfly-security/wildfly-elytron/blob/2.x/http/oidc/src/main/java/org/wildfly/security/http/oidc/TokenValidator.java#L85>



rsearls on Feb 17, 2025

Contributor Author

Its more straight forward to take the value from idToken which has been validated

fjuma commented on Feb 11, 2025 • edited

Contributor

@rsearls Thanks for working on this! It would also be good to add some unit tests for the case where the ID token contains the correct nonce and the case where the ID token contains the wrong nonce.

fjuma commented on Feb 11, 2025

Contributor

@rsearls Please update the base branch for this PR to the 2.6.x branch, thanks.



rsearls force-pushed the `JBEAP-28701-OIDC-Auth-Code` branch from `c4aec6e` to `3f02a79` last year

Compare

rsearls commented [on Feb 17, 2025](#)

Contributor


Author

All existing tests use the valid nonce case. I have add a test for the invalid case.

Once you are happy this the changes in this branch I will port them to 2.6.x

 **fjuma** requested changes [on Feb 20, 2025](#)

[View reviewed changes](#)

 **fjuma** left a comment

Contributor

Thanks [@rsearls](#)! I've added some comments, let me know if you have any questions.

`http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java`

Outdated

97	101		<code>protected String strippedOauthParametersRequestUri;</code>
98	102		
	103	+	<code>private int NONCE_SIZE = 36;</code>
	104	+	<code>private final String sessionId = generateSessionId();</code>

 **fjuma** [on Feb 20, 2025](#)

Contributor

Maybe we could name this `sessionRandomValue` or something like that?

 **fjuma** [on Feb 20, 2025](#)

Contributor

The random value can be generated when creating the authentication request.

 **rsearls** [on Feb 24, 2025](#)

Contributor

Author

Variable renamed.

There are several reasons I made sessionId private final in class scope rather than a method local variable. I wanted to keep the needed code changes to this class to a minimum. The variable is used in 3 different methods, getRedirectUri, createRequestWithRequestParameter, convertToRequestParameter.

Each method would require a signature change. The methods are called in 5 different places also requiring a change.

I also thought that in the future some calling class might need access to the value of sessionId. Having a class scope private final variable would enable a consistent accurate reference.

However I can make the change you requested if you prefer.



fjuma on Mar 6, 2025 • edited ▾

Contributor

We should be using a different random value for each authentication request. In loginRedirect, I think you could initialize the variable, just like the state variable is initialized there and then pass it to getRedirectUri and the other methods you mentioned. These methods are not public API so it's ok to update the signatures.



rsearls on Mar 6, 2025

Contributor

Author

done

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java

Outdated

224	231		redirectUriBuilder.addParameter(RESPONSE_TYPE, CODE)
225		-	.addParameter(CLIENT_ID, deployment.getResourceName())
	232	+	.addParameter(CLIENT_ID, deployment.getResourceName())
	233	+	.addParameter(NONCE, String.valueOf(sessionId.hashCode()))



fjuma on Feb 20, 2025

Contributor

Here, we need to use a cryptographic hash of the random value. We can use

`MessageDigest` for this.



rsearls on Feb 25, 2025

Contributor

Author

done

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java

Outdated

Show resolved

```
http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java
```

Outdated

```
338     348     }  
339     -     if (!state.equals(stateCookieValue)) {  
349     +  
350     +     String sCookieValue = stateCookieValue;
```

**fjuma** on Feb 20, 2025

Contributor

Why are these changes needed?

The `checkStateCookie()` method currently deals specifically with the `deployment.getStateCookieName()` (i.e., the `OAuth-Token-Request-State` cookie).

**fjuma** on Mar 6, 2025

Contributor

I think this still needs to be addressed. The state cookie is something separate that's unrelated to the new cookie that's being introduced.

**rsearls** on Mar 6, 2025

Contributor

Author

When more than 1 cookie is set in `exchange.getResponse()` (see line 324-326) they are returned in the request as a string of concatenated text in this format: `1st-cookie-value; 2nd-cookie-name=2nd-cookie-value; .. etc.` This check is evaluating "stateCookieValue" which is part of the pre-existing code. I have changed the initial variable name to be more generic. I think the original variable name should remain for consistency and clarity.

**fjuma** on Mar 6, 2025 • edited

Contributor

That doesn't sound right. There should be an `ArrayList` that contains 2 separate `HttpServerCookies`, each with their own values. That's why changes should not be needed to anything that references the other cookie, its value should be unchanged.

Is it possible the concatenation stuff you mentioned is due to changes made to the test itself?

**rsearls** on Mar 8, 2025

Contributor

Author

`okhttp3.mockwebserver.RecordedRequest` appears to only return headers. For "Cookie" it is of the format described. I made changes in `AbstractBaseHttpTest` to parse this and provide an array of cookies as needed.

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java

Outdated

```

445 | 462 |           idToken = verifiedTokens.getIdToken();
446 | 463 |           token = verifiedTokens.getAccessToken();
    | 464 | +
    | 465 | +           String stateCookieValue = getCookieValue(deployment.getStateCookieName());

```



fjuma on Feb 20, 2025 • edited

Contributor

Won't this get the value of the `OAuth-Token-Request-State` cookie instead of the session random value cookie?



rsearls on Feb 24, 2025

Contributor

Author

This is related to the issue described for line 350.

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java

Outdated

```

    | 467 | +           String sessionIdValue = "";
    | 468 | +           for(int i=0; i < cookieArr.length; i++) {
    | 469 | +               String cookie = cookieArr[i].trim();
    | 470 | +               if (cookie.startsWith(SESSION_ID+"=")) {

```



fjuma on Feb 20, 2025 • edited

Contributor

Just to check, is this needed? I don't see a similar check being done in the code that obtains the state cookie value.



rsearls on Feb 24, 2025 • edited

Contributor

Author

Cookie state is performed by the challenge returned at line 428 (i.e `checkStateCookie()`). This is needed to get at the value for the `session_id` as described for line 350

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java

Outdated

```

    | 473 | +           }
    | 474 | +           }
    | 475 | +           String nonceValue = idToken.getNonce();
    | 476 | +           if (nonceValue == null || !nonceValue.equals(String.valueOf(

```



fjuma on Feb 20, 2025

Contributor

Here, we should use the cryptographic hash as mentioned above.



fjuma on Feb 20, 2025 • edited ▾

Contributor

Because the nonce validation is part of verifying the ID token, I think it makes sense for this check to be done in the OIDC `TokenValidator#parseAndVerifyToken` method. From the `TokenValidator` we have access to the `oidcClientConfiguration` from which we can get the value of the session random value cookie and we can get the nonce from `idJwtClaims`.



rsearls on Feb 25, 2025

Contributor

Author

done

`http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java`

Outdated

549	584	jwtClaims.setClaim(REDIRECT_URI, redirectUri);
550	585	jwtClaims.setClaim(RESPONSE_TYPE, CODE);
551	586	jwtClaims.setClaim(CLIENT_ID, deployment.getResourceName());
	587	+ jwtClaims.setClaim(NONCE, String.valueOf(sessionId.hashCode()));



fjuma on Feb 20, 2025

Contributor

Note, same comment as above regarding using a cryptographic hash.



rsearls on Feb 25, 2025

Contributor

Author

done

`http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java`

Outdated

663	+	SecureRandom random = new SecureRandom();
664	+	byte[] nonceData = new byte[NONCE_SIZE];
665	+	random.nextBytes(nonceData);
666	+	return String.valueOf(ByteIterator.ofBytes(nonceData)



fjuma on Feb 20, 2025

Contributor

I think this can be `return`
`ByteIterator.ofBytes(nonceData).base64Encode().drainToString();`



rsearls on Feb 25, 2025

Contributor

Author

done

```
http/oidc/src/test/java/org/wildfly/security/http/oidc/OidcTest.java
```

Show resolved

rsearls force-pushed the `JBEAP-28701-OIDC-Auth-Code` branch from `3f02a79` to `d6f32ce` last year

Compare

fjuma reviewed on Mar 6, 2025

View reviewed changes

```
http/oidc/src/main/java/org/wildfly/security/http/oidc/Oidc.java
```

Outdated

```

456 | + | md.update(src.getBytes());
457 | + | return new String(md.digest(), StandardCharsets.UTF_8);
458 | + | } catch (NoSuchAlgorithmException e) {
459 | + |

```

fjuma on Mar 6, 2025 Contributor

We should use `throw log...` here.

rsearls on Mar 6, 2025 Contributor Author

done

fjuma reviewed on Mar 6, 2025

View reviewed changes

```
http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java
```

Outdated

```

224 | 232 | redirectUriBuilder.addParameter(RESPONSE_TYPE, CODE)
225 | - | .addParameter(CLIENT_ID, deployment.getResourceName())
233 | + | .addParameter(CLIENT_ID, deployment.getResourceName())
234 | + | .addParameter(NONCE, String.valueOf(cryptoValue));

```

fjuma on Mar 6, 2025 Contributor

Since `cryptoValue` is already a `String`, `String.valueOf` isn't needed.

rsearls on Mar 6, 2025 Contributor Author

done



fjuma reviewed [on Mar 6, 2025](#)

[View reviewed changes](#)

http/oidc/src/main/java/org/wildfly/security/http/oidc/Oidc.java Outdated

```

453 + public static String getCryptographicValue(final String src) {
454 +     try {
455 +         MessageDigest md = MessageDigest.getInstance(SHA256);
456 +         md.update(src.getBytes());

```

fjuma [on Mar 6, 2025](#) Contributor

getBytes(StandardCharsets.UTF_8)

rsearls [on Mar 6, 2025](#) Contributor Author

done



fjuma reviewed [on Mar 6, 2025](#)

[View reviewed changes](#)

http/oidc/src/main/java/org/wildfly/security/http/oidc/Oidc.java Outdated

```

454 +     try {
455 +         MessageDigest md = MessageDigest.getInstance(SHA256);
456 +         md.update(src.getBytes());
457 +         return new String(md.digest(), StandardCharsets.UTF_8);

```

fjuma [on Mar 6, 2025](#) • edited Contributor

Here, I think we could use

```

ByteIterator.ofBytes(md.digest()).base64Encode(BASE64_URL,
false).drainToString()

```

rsearls [on Mar 6, 2025](#) Contributor Author

done



fjuma reviewed [on Mar 6, 2025](#)



View reviewed changes

```

http/oidc/src/main/java/org/wildfly/security/http/oidc/TokenValidator.java
ava
88 +         return parseAndVerifyToken(idToken, accessToken, null);
89 +     }
90 +
91 +     public VerifiedTokens parseAndVerifyToken(final String idToken, final

```



fjuma on Mar 6, 2025

Contributor

I don't think the method signature needs to be changed. We can get the session cookie value using the `clientConfiguration` variable.



rsearls on Mar 6, 2025

Contributor

Author

`OidcClientConfiguration` does not retain a reference to `OidcHttpFacade` or any object that references `OidcHttpFacade`, which is required to get access the the request's cookies. The value must be passed in to the method.



fjuma on Mar 6, 2025

Contributor

Ah, I see. Another option could be to pass the `OidcHttpFacade` along with the `OidClientConfiguration` when instantiating the validator. That way we don't need to pass the value to the `parseAndVerifyToken` method and it can instead use the facade to get the value it needs to use for validation like it uses the `OidcClientConfiguration` to get other needed values.



rsearls on Mar 8, 2025

Contributor

Author

done. `OidClientConfiguration` is not needed.



fjuma reviewed on Mar 6, 2025

View reviewed changes

```

http/oidc/src/main/java/org/wildfly/security/http/oidc/TokenValidator.java
ava
88 | 94 |         jwtConsumerBuilder.setExpectedAudience(clientConfiguration.c
89 | 95 |         jwtConsumerBuilder.registerValidator(new AzpValidator(client
90 | 96 |         jwtConsumerBuilder.registerValidator(new AtHashValidator(acc
97 | + |         if (stateCookieValue != null) {

```



fjuma on Mar 6, 2025

Contributor

Since the state cookie value refers to something else we should be using a different variable name here.



rsearls on Mar 6, 2025

Contributor

Author

I provided a more generic name



rsearls force-pushed the `JBEAP-28701-OIDC-Auth-Code` branch from `d6f32ce` to `c13e1c1` last year

Compare



fjuma reviewed on Mar 6, 2025

View reviewed changes

`http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java`

Outdated

```

550 | 572 |           jwtClaims.setClaim(RESPONSE_TYPE, CODE);
551 | 573 |           jwtClaims.setClaim(CLIENT_ID, deployment.getResourceName());
    | 574 | +         String cryptoValue = Oidc.getCryptographicValue(sessionRandomVa
    | 575 | +         jwtClaims.setClaim(NONCE, String.valueOf(cryptoValue));

```



fjuma on Mar 6, 2025

Contributor

`String.valueOf` can be removed here



fjuma on Mar 6, 2025 • edited

Contributor

Just thinking, could we pass the crypto value directly to the `convertToRequestParameter` method instead of the session random value?



rsearls on Mar 6, 2025

Contributor

Author

done



fjuma reviewed on Mar 6, 2025

View reviewed changes

http/oidc/src/main/java/org/wildfly/security/http/oidc/ElytronMessages.java

Outdated

```

280 | 280 | RuntimeException invalidAuthenticationRequestFormat();
    | 281 | +
    | 282 | + @Message(id = 23071, value = "Invalid %s")
    | 283 | + String invalidSessionRandomValue(String name);

```



fjuma on Mar 6, 2025 • edited

Contributor

Maybe we could rename this to invalidNonceValue(String nonce) and update the message itself to "Invalid ID token nonce %s".



rsearls on Mar 8, 2025

Contributor

Author

done



fjuma reviewed on Mar 6, 2025

[View reviewed changes](#)

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java

Outdated

```

352 | + if (cookiesStr != null) {
353 | +     String[] cookieArr = cookiesStr.split(";");
354 | +     stateCookieValue = cookieArr[0];
355 | + }

```



fjuma on Mar 6, 2025

Contributor

This shouldn't be needed.



rsearls on Mar 8, 2025

Contributor

Author

Changes to AbstractBaseHttpTest resolved this



fjuma reviewed on Mar 6, 2025

[View reviewed changes](#)

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java

Outdated

```

442 | 460 | try {

```

443	461		TokenValidator tokenValidator = TokenValidator.builder(depl
444		-	TokenValidator.VerifiedTokens verifiedTokens = tokenValidato
	462	+	String stateCookieValue = getCookieValue(deployment.getState



fjuma on Mar 6, 2025 • edited ▾

Contributor

We should be using `String sessionRandomValue = getCookieValue(SESSION_RANDOM_VALUE)` to get the value of the right cookie.



rsearls on Mar 8, 2025

Contributor

Author

Changed parseAndVerifyToken per previous comment



fjuma reviewed on Mar 6, 2025

[View reviewed changes](#)

```
http/oidc/src/main/java/org/wildfly/security/http/oidc/TokenValidator.j
ava
```

Outdated

290	299		
	300	+	
	301	+	private static class NonceValidator implements ErrorCodeValidator {
	302	+	private final String stateCookieValue;



fjuma on Mar 6, 2025

Contributor

Maybe sessionRandomCookieValue might be better to use to avoid confusion with the state cookie.



rsearls on Mar 6, 2025

Contributor

Author

done



rsearls on Mar 8, 2025

Contributor

Author

changed per previous comments



fjuma reviewed on Mar 6, 2025

[View reviewed changes](#)

```
http/oidc/src/main/java/org/wildfly/security/http/oidc/TokenValidator.j
ava
```

Outdated

```

309 + JwtClaims idJwtClaims = jwtContext.getJwtClaims();
310 + IDToken idToken = new IDToken(idJwtClaims);
311 +
312 + String[] cookieArr = stateCookieValue.split(";");

```



fjuma on Mar 6, 2025

Contributor

As mentioned above, this shouldn't be needed.



rsearls on Mar 8, 2025

Contributor

Author

done



fjuma reviewed on Mar 6, 2025

[View reviewed changes](#)

http/oidc/src/test/java/org/wildfly/security/http/oidc/OidcBaseTest.java Outdated

```

a
437 + if (tmpCookies.get(i).getName().equals(oidcClient
438 + stateCookie = tmpCookies.get(i);
439 + } else if (tmpCookies.get(i).getName().equals(ST
440 + sessionIdStr = ";" + tmpCookies.get(i).getN

```



fjuma on Mar 6, 2025

Contributor

I'm wondering if the changes in this method are causing the concatenation issue you mentioned above.



rsearls on Mar 8, 2025

Contributor

Author

No this is not the issue



fjuma reviewed on Mar 6, 2025

[View reviewed changes](#)

http/oidc/src/test/java/org/wildfly/security/http/oidc/OidcTest.java Outdated

```

377 + }
378 +
379 + @Test
380 + public void testtestOpenIDScopeNONCE() throws Exception {

```



fjuma on [Mar 6, 2025](#)

Contributor

s/testtest/test

We should still be testing the mismatch case here.



rsearls on [Mar 8, 2025](#)

Contributor

Author

done



fjuma reviewed on [Mar 6, 2025](#)

[View reviewed changes](#)

`http/oidc/src/test/java/org/wildfly/security/http/oidc/OidcTest.java` Outdated

```

378 +
379 +     @Test
380 +     public void testtestOpenIDScopeNONCE() throws Exception {
381 +         String expectedScope = OIDC_SCOPE;

```



fjuma on [Mar 6, 2025](#)

Contributor

We don't need to test the expected scope here. The main idea is to just use configuration that doesn't make use of the request parameter so we can test what happens when a normal authentication request is A standard config like `getOidcConfigurationInputStreamWithProviderUrl` could be used.



rsearls on [Mar 8, 2025](#)

Contributor

Author

done



fjuma reviewed on [Mar 6, 2025](#)

[View reviewed changes](#)

`http/oidc/src/main/java/org/wildfly/security/http/oidc/TokenValidator.java` Outdated

```

321 +     }
322 +     String nonceValue = idToken.getNonce();
323 +     if (nonceValue == null || !MessageDigest.isEqual(nonceValue
324 +         sessionIdValue.getBytes())) {

```



fjuma on [Mar 6, 2025](#)

Contributor

We should be able to use `sessionRandomValue.equals(nonceValue)`



fjuma reviewed on [Mar 6, 2025](#)

[View reviewed changes](#)

http/oidc/src/main/java/org/wildfly/security/http/oidc/TokenValidator.java Outdated

89	95		<code>jwtConsumerBuilder.registerValidator(new AzpValidator(client</code>
90	96		<code>jwtConsumerBuilder.registerValidator(new AtHashValidator(acc</code>
	97	+	<code>if (cookiesStr != null) {</code>
	98	+	<code>jwtConsumerBuilder.registerValidator(new NonceValidator</code>



fjuma on [Mar 6, 2025](#)

Contributor

The `if` here shouldn't be needed. Since we are now always sending the nonce in the authentication request, this validator should always be registered.



rsearls force-pushed the `JBEAP-28701-OIDC-Auth-Code` branch from `c13e1c1` to `755ccf4` last year

[Compare](#)



fjuma reviewed on [Mar 10, 2025](#)

[View reviewed changes](#)

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java Outdated

182	188		<code>}</code>
183	189		
184		-	<code>protected String getRedirectUri(String state) {</code>
	190	+	<code>protected String getRedirectUri(String state, <u>String cryptoValue</u>) {</code>



fjuma on [Mar 10, 2025](#)

Contributor

I think it might be good to rename `cryptoValue` here to something like `sessionRandomValueHash`



fjuma on [Mar 10, 2025](#)

Contributor

We could also just name it nonce.



rsearls on [Mar 10, 2025](#)

Contributor Author

done



fjuma reviewed on [Mar 10, 2025](#)

[View reviewed changes](#)

`http/oidc/src/main/java/org/wildfly/security/http/oidc/ElytronMessages.java`

Outdated

282	+	@Message(id = 23071, value = "Invalid ID token nonce: %s")
283	+	String invalidNonceValue(String name);
284	+	
285	+	@Message(id = 23072, value = "No Such algorithm: '%s'")



fjuma on [Mar 10, 2025](#)

Contributor

s/Such/such



rsearls on [Mar 10, 2025](#)

Contributor Author

done

65 hidden items

[Load more...](#)



fjuma reviewed on [Mar 10, 2025](#)

[View reviewed changes](#)

`http/oidc/src/main/java/org/wildfly/security/http/oidc/Oidc.java`

Outdated

445	452	return true;
446	453	}
447	454	
448	455	+ public static String getCryptographicValue(final String src) {



fjuma on [Mar 10, 2025](#)

Contributor

Does this need to be public?



rsearls on [Mar 10, 2025](#)

Contributor Author

Yes it is referenced by TokenValidator and OidcRequestAuthenticator



fjuma on [Mar 10, 2025](#)

Contributor

Could it be protected instead?



rsearls on [Mar 10, 2025](#)

Contributor Author

If I move it into OidcHttpFacade it could be made public and accessible to TokenValidator and OidcRequestAuthenticator.

Would you prefer that?



fjuma on [Mar 10, 2025](#)

Contributor

It's fine to have utility methods in Oidc.java but we typically make them protected where it makes sense to do so.



rsearls on [Mar 10, 2025](#)

Contributor Author

done



fjuma reviewed on [Mar 10, 2025](#)

[View reviewed changes](#)

`http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java`

Outdated

442	453	try {
443	454	TokenValidator tokenValidator = TokenValidator.builder(depl
444	-	TokenValidator.VerifiedTokens verifiedTokens = tokenValidat
	455	String sessionRandValueStr = getCookieValue(SESSION_RANDOM



fjuma on [Mar 10, 2025](#)

Contributor

I think this line can be removed now, I don't see sessionRanomValueStr being used.



rsearls on [Mar 10, 2025](#)

Contributor Author

done



fjuma reviewed [on Mar 10, 2025](#)

[View reviewed changes](#)

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java Outdated

536	551	}
537	552	
538		- private String convertToRequestParamer(URIBuilder redirectUriBuild
	553	+ private String convertToRequestParamer(URIBuilder redirectUriBuild

fjuma [on Mar 10, 2025](#) Contributor

Same comment here about cryptoValue, would be good to rename.

rsearls [on Mar 10, 2025](#) Contributor Author

done



fjuma reviewed [on Mar 10, 2025](#)

[View reviewed changes](#)

http/oidc/src/main/java/org/wildfly/security/http/oidc/TokenValidator.java Outdated

83	85	* @throws OidcException if the ID token is invalid
84	86	*/
85	87	public VerifiedTokens parseAndVerifyToken(final String idToken, final
	88	+ return parseAndVerifyToken(idToken, accessToken, null);

fjuma [on Mar 10, 2025](#) Contributor

Just wondering if this variant without the facade is needed. We should always be validating the nonce.

rsearls [on Mar 10, 2025](#) Contributor Author

BearerTokenRequestAuthenticator and RefreshableOidcSecurityContext call parseAndVerifyToken only RefreshableOidcSecurityContext appears to need the param change.

done



fjuma reviewed [on Mar 10, 2025](#)

[View reviewed changes](#)

```
http/oidc/src/main/java/org/wildfly/security/http/oidc/TokenValidator.java
309 + IDToken idToken = new IDToken(idJwtClaims);
310 +
311 + OidcHttpFacade.Cookie cookie = this.facade.getRequest().getCookie();
312 + if (cookie != null) {
```



fjuma [on Mar 10, 2025](#)

Contributor

Since we should always be sending the nonce in the request, if the cookie is null, I think the validator should fail.



rsearls [on Mar 10, 2025](#)

Contributor

Author

done



rsearls [force-pushed](#) the `JBEAP-28701-OIDC-Auth-Code` branch from `755ccf4` to `78bcee3` [last year](#)

[Compare](#)



fjuma reviewed [on Mar 10, 2025](#)

[View reviewed changes](#)

```
http/oidc/src/main/java/org/wildfly/security/http/oidc/RefreshableOidcSecurityContext.java Outdated
39 | 40 | }
40 | 41 |
41 | - | public RefreshableOidcSecurityContext(OidcClientConfiguration clientConfiguration, OidcClientConfiguration clientConfiguration) {
42 | + | public RefreshableOidcSecurityContext(OidcClientConfiguration clientConfiguration, OidcClientConfiguration clientConfiguration) {
```



fjuma [on Mar 10, 2025](#)

Contributor

Just wondering, is it possible to pass in the cookie here instead of the facade?



rsearls [on Mar 10, 2025](#)

Contributor

Author

done



rsearls force-pushed the `JBEAP-28701-OIDC-Auth-Code` branch from `78bcee3` to `756cddb` last year

[Compare](#)



fjuma reviewed [on Mar 11, 2025](#)

[View reviewed changes](#)

http/oidc/src/main/java/org/wildfly/security/http/oidc/TokenValidator.java Outdated

```

304 + IDToken idToken = new IDToken(idJwtClaims);
305 +
306 +     if (cookie != null) {
307 +         String sessionIdValue = Oidc.getCryptographicValue(cookie);

```

fjuma on Mar 11, 2025 • edited Contributor

This is a very minor comment, would be good to rename sessionIdValue to sessionRandomValueHash.

rsearls on Mar 11, 2025 Contributor Author

done



fjuma reviewed [on Mar 11, 2025](#)

[View reviewed changes](#)

http/oidc/src/main/java/org/wildfly/security/http/oidc/TokenValidator.java Outdated

```

308 + String nonceValue = idToken.getNonce();
309 +     if (nonceValue == null || !sessionIdValue.equals(nonceValue)) {
310 +         return new ErrorCodeValidator.Error(INVALID_SESSION_ID, "Invalid session ID");
311 +         log.invalidNonceValue(nonceValue == null ? "nonce is null" : "nonce does not match session ID");

```

fjuma on Mar 11, 2025 Contributor

I don't think specifying "null" explicitly is needed here.

rsearls on Mar 11, 2025 Contributor Author

done



rsearls force-pushed the `JBEAP-28701-OIDC-Auth-Code` branch 2 times, most recently from `7e00fe2` to `57ed6d6` [last year](#)

[Compare](#)



fjuma reviewed [on Mar 13, 2025](#)

[View reviewed changes](#)

```

http/oidc/src/main/java/org/wildfly/security/http/oidc/OidcRequestAuthenticator.java Outdated
224 | 230 |      redirectUriBuilder.addParameter(RESPONSE_TYPE, CODE)
225 | -   |      .addParameter(CLIENT_ID, deployment.getResourceName())
    | 231 | +   |      .addParameter(CLIENT_ID, deployment.getResourceName())
    | 232 | +   |      .addParameter(NONCE, sessionRandomValueHash);

```



fjuma [on Mar 13, 2025](#)

Contributor

I don't think we should do this here. I just realized that for the REQUEST and REQUEST_URI cases below, this will result in the nonce being added to both the redirectUriBuilder and to the JWT claims. I think `addParameter(NONCE, sessionRandomValueHash);` should be called from `createOAuthRequest` instead.



rsearls [on Mar 14, 2025](#)

Contributor

Author

done



fjuma reviewed [on Mar 13, 2025](#)

[View reviewed changes](#)

```

http/oidc/src/test/java/org/wildfly/security/http/oidc/OidcTest.java Outdated
369 | 369 |
    | 370 | +   | @Test
    | 371 | +   | // Generate an invalid sessionRandomValue so that the nonce check fo
    | 372 | +   | public void testSessionIdNonceMismatch() throws Exception {

```



fjuma [on Mar 13, 2025](#)

Contributor

Would be good to rename to `testRequestParameterNonceMismatch` and to also add one more test method called `testRequestUriParameterNonceMismatch` that uses `getOidcConfigurationInputStreamWithRequestParameter(REQUEST_URI.getValue())...`



rsearls on Mar 14, 2025

Contributor

Author

done



rsearls force-pushed the **JBEAP-28701-OIDC-Auth-Code** branch from **57ed6d6** to **76523e2** [last year](#)

[Compare](#)



fjuma approved these changes on Mar 14, 2025

[View reviewed changes](#)



fjuma left a comment

Contributor

Thanks for the updates [@rsearls](#), this looks good!

Please update the PR title and the commit message to reference an ELY issue instead of the JBEAP issue. Please also update the commit message to add some more details (e.g., "[ELY-XYZ] Add a nonce to OIDC requests for [CVE-2024-12369](#)" or something like that). Thanks.



fjuma requested a review from **darranl** [last year](#)



rsearls changed the title **[JBEAP-28701] added use of nonce [ELY-2887] Add a nonce to OIDC requests for CVE-2024-12369** on Mar 14, 2025



[ELY-2887] Add a nonce to OIDC requests for [CVE-2024-12369](#)

✓ [236003a](#)



rsearls force-pushed the **JBEAP-28701-OIDC-Auth-Code** branch from **76523e2** to **236003a** [last year](#)

[Compare](#)



fjuma added the **+1 FJ** label on Mar 17, 2025

darranl commented on Apr 13, 2025

Contributor

@rsearls I think we can close this one now as the maintenance issue was merged including forward merging to the upstream branches?



rsearls closed this on Apr 13, 2025

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

Reviewers



fjuma



skyllarr



darranl



Assignees

No one assigned

Labels

+1 FJ

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants

