Unauthorized access to Code With Me traffic (CVE-2021-25755)

Apr 2, 2021

In this post I am going to share some details about Code With Me traffic interception vulnerability CVE-2021-25755. Code With Me is a new collaborative development and pair programming service from JetBrains that provides such experience *just one click away*.

Short description:

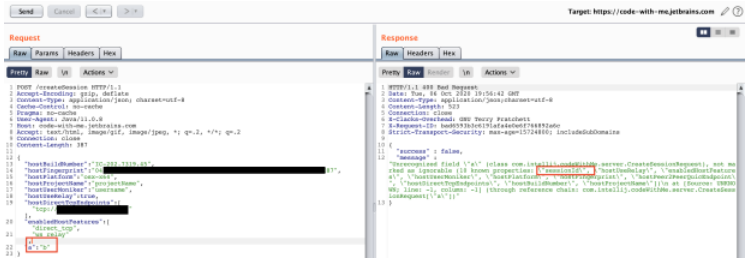
In JetBrains Code With Me before 2020.3, an attacker on the local network, knowing a session ID, could get access to the encrypted traffic.

Links:

- JetBrains Security Bulletin Q4 2020
- CVE-2021-25755
- CWM-1067
- JetBrains Coordinated Disclosure Policy

Details:

I intercepted Code With Me traffic and found the following request to create a new session. I slightly changed it to an see error message in response:

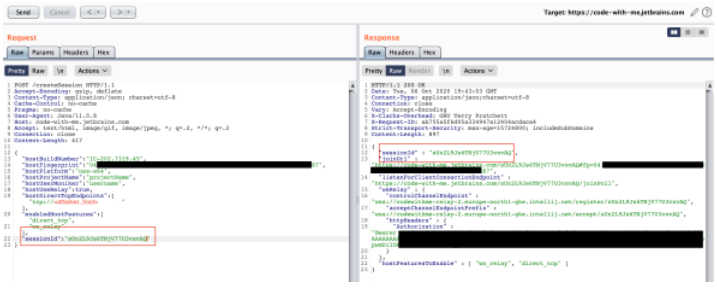


It turned out that it was possible to replace TCP endpoint hosts for existing sessions. The main problem here is that it was possible to define session for `createSession` request and replace existing session with another one but define different TCP host for the new session using information from the invitation link only:

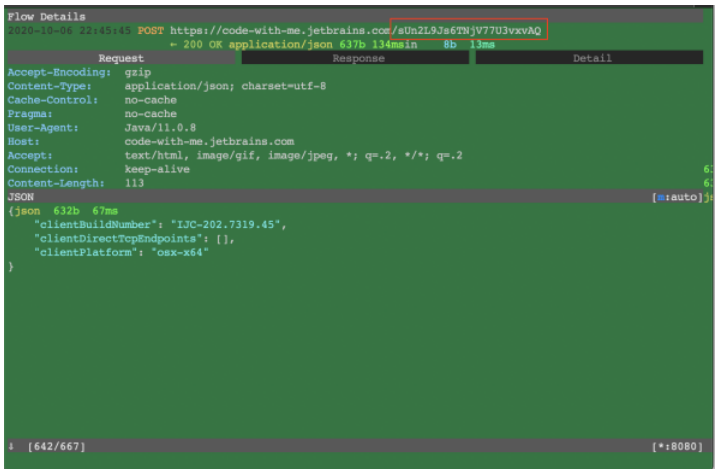
1. Host generates the invitation link and share it with other participants
2. Attacker takes this invitation link with `session id` and `fingerprint` in parameters:

   ```
   https://code-with-me.jetbrains.com/sUn2L9Js6TNjV77U3vxvAQ#p=IC&
   fp=0432495F97E9FBD672266015DD1E3E3361BAEFAA0E16E8CA47BEA23A39136E87
   ```

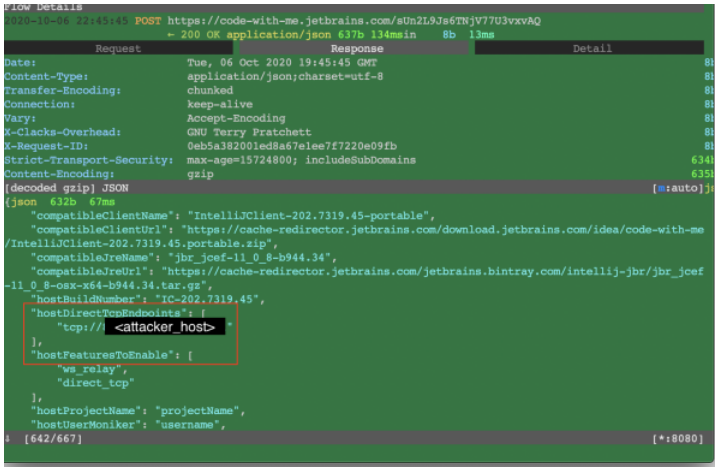
3. Attacker updates current session properties with `sessionId` parameter and set `hostDirectTcpEndpoints` to attacker's host with TCP proxy `"hostDirectTcpEndpoints" : [ "tcp://<attacker_host>:<port>"]` using `sessionId` and `hostFingerprint` from the invitation link:

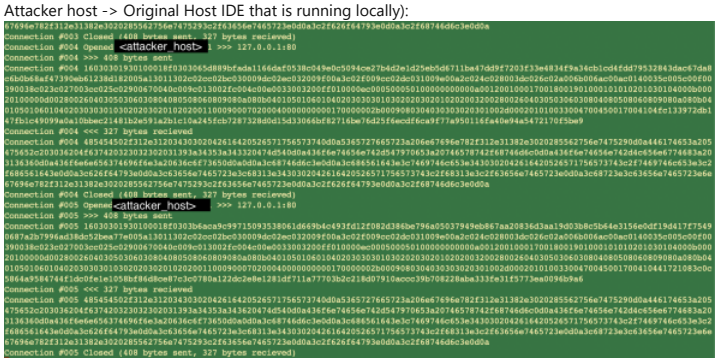
4. Victims follow this link to connect to the Host, but instead it connects to the attacker's host (which could proxy "Code With Me" traffic to a legitimate Host). Victim starts connection process and request details using the invitation link:



Victim receives an attacker host for connection:



5. Attacker intercepts encrypted traffic between the victims and legitimate Host (Victim's IDE -> Attacker host -> Original Host IDE that is running locally):



Timeline:

1. 6 Oct 2020 - reported to JetBrains (CWM-1067)
2. 7 Oct 2020 - confirmed
3. 1 Nov 2020 - fixed
4. 3 Feb 2021 - mentioned in JetBrains Security Bulletin, CVE assigned

---

Jay From Future's Blog (but not about future or futures)

Jay From Future's Blog (but not about future or futures)
jay.from.future@gmail.com

jay-from-future

Dark times lie ahead of us and there will be a time when we must choose between what is easy and what is right. (Albus Dumbledore, Harry Potter and the Goblet of Fire)