

2021-08-25 -CVE-2021-26084 -Confluence Server Webwork OGNL injection

漏洞-CVE-2021-26084

影响

主题	CVE-2021-26084 - Confluence Webwork OGNL注入
安全信息发布时间	25 Aug 2021
涉及产品	Confluence Server Confluence Data Center
影响Confluence版本	• All 4. x. x versions • All 5. x. x versions • All 6. 0. x versions • All 6. 1. x versions • All 6. 2. x versions • All 6. 3. x versions • All 6. 4. x versions • All 6. 5. x versions • All 6. 6. x versions • All 6. 7. x versions • All 6. 8. x versions • All 6. 9. x versions • All 6. 10. x versions • All 6. 11. x versions • All 6. 12. x versions • All 6. 13. x versions before 6. 13. 23 • All 6. 14. x versions • All 6. 15. x versions • All 7. 0. x versions • All 7. 1. x versions • All 7. 2. x versions • All 7. 3. x versions • All 7. 4. x versions before 7. 4. 11 • All 7. 5. x versions • All 7. 6. x versions • All 7. 7. x versions • All 7. 8. x versions • All 7. 9. x versions • All 7. 10. x versions • All 7. 11. x versions before 7. 11. 6 • All 7. 12. x versions before 7. 12. 5
修复版本	• 6. 13. 23 • 7. 4. 11 • 7. 11. 6 • 7. 12. 5 • 7. 13. 0

升级到版本6. 13. 23、7. 11. 6、7. 12. 5、7. 13. 0或7. 4. 11的客户不受影响

解决方案

方案一

升级到安全版本

方案二（临时）

执行以下脚本，对系统中的文件进行修正来临时解决注入的风险

[cve-2021-26084-update.sh](#)

安全漏洞描述

存在OGNL注入漏洞，该漏洞允许经过身份验证的用户（在某些情况下是未经身份验证的用户）在Confluence实例上执行任意代码。

方案二说明

就是将页面中\$actionKey之类的值进行固化，减少注入的可能。目前只对可以进行固化的页面信息进行了替换处理，但并未从源头进行处理。

查看脚本内容

```
#!/bin/bash
# Filename      : cve-2021-26084-update.sh
# Description: Temporary workaround for CVE-2021-26084 for Confluence instances
running on Linux based Operating Systems
# Reference     : https://confluence.atlassian.com/display/DOC
/Confluence+Security+Advisory+-+2021-08-25
# Usage        : sh cve-2021-26084-update.sh
# Version      : 1.4
set -u

# #####
# Update user specific data in this section

# set this to where Confluence is installed
# e.g. INSTALLATION_DIRECTORY=/opt/atlassian/confluence
INSTALLATION_DIRECTORY=/opt/atlassian/confluence

# #####
# Do not change anything below this line

if [ -z "$INSTALLATION_DIRECTORY" ]
then
    echo "Please set INSTALLATION_DIRECTORY within this script and try running this
script again.";
    exit 1;
fi

# Make sure we are running as the correct Linux user
if [ ! -w "$INSTALLATION_DIRECTORY/confluence" ]
then
    echo "ERROR: Please run this script as the Linux user that owns the
$INSTALLATION_DIRECTORY/confluence directory"
    echo " (i.e. " `ls -ld "$INSTALLATION_DIRECTORY/confluence" | awk '{ print $3
}' `")";
    exit 1;
fi
```

```

# Change SED flags dependent on OS
SEDFLAGS=-ri.bak
if uname -a | grep -qi "Darwin"
then
    SEDFLAGS=-Ei.bak
fi

# Change to Install Directory
echo "chdir '$INSTALLATION_DIRECTORY'"
cd "$INSTALLATION_DIRECTORY";
if [ $? -ne 0 ]; then
    echo "ERROR: Failed to change to the directory $INSTALLATION_DIRECTORY!"
    exit 1;
fi
echo ""

# check zip/unzip dependencies up front
UNZIP=`which unzip`
ZIP=`which zip`
if [ -z "$ZIP" ]
then
    echo "ERROR: 'zip' package is missing. Please install 'zip' and try running
this update script again.";
    echo "e.g. RHEL based OS          , try 'sudo yum install zip unzip'"
    echo "e.g. Ubuntu/Docker based OS, try (as root) 'apt update; apt install zip
unzip'"
    echo "UPDATE FAILED, EXITING!"
    echo ""
    exit 1;
fi
if [ -z "$UNZIP" ]
then
    echo "ERROR: 'unzip' package is missing. Please install 'unzip' and try running
this update script again.";
    echo "e.g. RHEL based OS          , try 'sudo yum install zip unzip'"
    echo "e.g. Ubuntu/Docker based OS, try (as root) 'apt update; apt install zip
unzip'"
    echo "UPDATE FAILED, EXITING!"
    echo ""
    exit 1;
fi

# #####
# File 1 of 5

```

```

echo "File 1: 'confluence/users/user-dark-features.vm':"
echo -n "    a. backing up file.. "
cp -np confluence/users/user-dark-features.vm confluence/users/user-dark-features.
vm.original;
echo "done"
echo -n "    b. updating file.. "
sed $SEDFLAGS 's/(Enable dark feature.+value=) [^"]+/"\1featureKey"/' confluence
/users/user-dark-features.vm;
echo "done"
echo "    c. showing file changes.. "
diff confluence/users/user-dark-features.vm.original confluence/users/user-dark-
features.vm;
echo -n "    d. validating file changes.. "
if grep -qi "'\${!action.featureKey}'" confluence/users/user-dark-features.vm
then
    echo "ERROR: Failed to update confluence/users/user-dark-features.vm"
    echo ""
    echo "UPDATE FAILED, EXITING!"
    exit 1;
fi
if ! grep -qi "value=featureKey" confluence/users/user-dark-features.vm
then
    echo "ERROR: Failed to update confluence/users/user-dark-features.vm"
    echo ""
    echo "UPDATE FAILED, EXITING!"
    exit 1;
fi
echo "ok"
echo "    e. file updated successfully!"
echo ""

# #####
# File 2 of 5

echo "File 2: 'confluence/login.vm':"
echo -n "    a. backing up file.. "
cp -np confluence/login.vm confluence/login.vm.original;
echo "done"
echo -n "    b. updating file.. "
sed $SEDFLAGS 's/("Hidden" "name=. token. " "value=) [^"]+/"\1token"/' confluence
/login.vm;
echo "done"
echo "    c. showing file changes.. "

```

```

diff confluence/login.vm.original confluence/login.vm
echo -n "    d. validating file changes.. "
if grep -qi "'\${action.token}'" confluence/login.vm
then
    echo "ERROR: Failed to update confluence/login.vm"
    echo ""
    echo "UPDATE FAILED, EXITING!"
    exit 1;
fi
if ! grep -qi "value=token" confluence/login.vm
then
    echo "ERROR: Failed to update confluence/login.vm"
    echo ""
    echo "UPDATE FAILED, EXITING!"
    exit 1;
fi
echo "ok"
echo "    e. file updated successfully!"
echo ""

# #####
# File 3 of 5

echo "File 3: 'confluence/pages/createpage-entervariables.vm':"
echo -n "    a. backing up file.. "
cp -np confluence/pages/createpage-entervariables.vm confluence/pages/createpage-entervariables.vm.original;
echo "done"
echo -n "    b. updating file.. "
sed $SEDFLAGS 's/("Hidden" "name=. ([a-zA-Z]+). " "value=).\${!!}[^"]+/"\1\2"/'
confluence/pages/createpage-entervariables.vm;
echo "done"
echo "    c. showing file changes.."
diff confluence/pages/createpage-entervariables.vm.original confluence/pages
/createpage-entervariables.vm
echo -n "    d. validating file changes.."
if grep -qi "value='\${querystring}" confluence/pages/createpage-entervariables.vm
then
    echo "ERROR: Failed to update confluence/pages/createpage-entervariables.vm"
    echo ""
    echo "UPDATE FAILED, EXITING!"
    exit 1;
fi
if grep -qi "value='\${linkCreation}" confluence/pages/createpage-entervariables.vm

```

```

then
    echo "ERROR: Failed to update confluence/pages/createpage-entervariables.vm"
    echo ""
    echo "UPDATE FAILED, EXITING!"
    exit 1;
fi
if ! grep -qi "value=linkCreation" confluence/pages/createpage-entervariables.vm
then
    echo "ERROR: Failed to update confluence/pages/createpage-entervariables.vm"
    echo ""
    echo "UPDATE FAILED, EXITING!"
    exit 1;
fi
echo "ok"
echo "    e. file updated successfully!"
echo ""

# #####
# File 4 of 5

echo "File 4: 'confluence/template/custom/content-editor.vm':"
echo -n "    a. backing up file.. "
cp -np confluence/template/custom/content-editor.vm confluence/template/custom
/content-editor.vm.original;
echo "done"
echo -n "    b. updating file.. "
sed $SEDFLAGS 's/("Hidden" "name=. ([a-zA-Z]+). " "value=).\${!}["^"]+"/\1\2"/'
confluence/template/custom/content-editor.vm;
sed $SEDFLAGS 's/("Hidden" "id=sourceTemplateId.*value=)["^"]+"/\1templateId"/'
confluence/template/custom/content-editor.vm;
echo "done"
echo "    c. showing file changes.."
diff confluence/template/custom/content-editor.vm.original confluence/template
/custom/content-editor.vm
echo "    d. file updated successfully!"
echo ""

# #####
# File 5 of 5

CONFLUENCE_EDITOR_JAR=`ls -l confluence/WEB-INF/atlassian-bundled-plugins
/confluence-editor-loader*.jar 2> /dev/null`
echo "File 5: 'confluence/WEB-INF/atlassian-bundled-plugins/confluence-editor-
loader*.jar':"

```

```

if [ ! -z "$CONFLUENCE_EDITOR_JAR" ]
then
    echo "    a. extracting templates/editor-preload-container.vm from
$CONFLUENCE_EDITOR_JAR. . "
    export TMP_EXTRACT_DIR=.
    unzip -o -d $TMP_EXTRACT_DIR $CONFLUENCE_EDITOR_JAR templates/editor-preload-
container.vm;
    if [ -f templates/editor-preload-container.vm ]
    then
        cp -np $TMP_EXTRACT_DIR/templates/editor-preload-container.vm
$TMP_EXTRACT_DIR/templates/editor-preload-container.vm.original;

        echo -n "    b. updating file.. "
        sed $SEDFLAGS 's/("Hidden" "id=syncRev.*value=) [^"]+("/\1syncRev"/'
$TMP_EXTRACT_DIR/templates/editor-preload-container.vm;
        echo "done"
        echo "    c. showing file changes.."
        diff $TMP_EXTRACT_DIR/templates/editor-preload-container.vm.original
$TMP_EXTRACT_DIR/templates/editor-preload-container.vm;

        echo -n "    d. validating file changes.. "
        if grep -qi "action.syncRev" $TMP_EXTRACT_DIR/templates/editor-preload-
container.vm
        then
            echo "ERROR: Failed to update $TMP_EXTRACT_DIR/templates/editor-preload-
container.vm"
            echo ""
            echo "UPDATE FAILED, EXITING!"
            exit 1;
        fi
        if ! grep -qi "value=syncRev" $TMP_EXTRACT_DIR/templates/editor-preload-
container.vm
        then
            echo "ERROR: Failed to update $TMP_EXTRACT_DIR/templates/editor-preload-
container.vm"
            echo ""
            echo "UPDATE FAILED, EXITING!"
            exit 1;
        fi
        echo "ok"

        echo -n "    e. updating $CONFLUENCE_EDITOR_JAR with $TMP_EXTRACT_DIR
/templates/editor-preload-container.vm. . "
        zip "$CONFLUENCE_EDITOR_JAR" $TMP_EXTRACT_DIR/templates/editor-preload-

```

```

container.vm;
    ls -l "$CONFLUENCE_EDITOR_JAR";

    echo -n "    f. cleaning up temp files.."
    rm -f $TMP_EXTRACT_DIR/templates/editor-preload-container.vm
$TMP_EXTRACT_DIR/templates/editor-preload-container.vm.bak $TMP_EXTRACT_DIR
/templates/editor-preload-container.vm.original;
    echo "ok"

    echo "    g. extracting templates/editor-preload-container.vm from
$CONFLUENCE_EDITOR_JAR again to check changes within JAR.. "
    export TMP_EXTRACT_DIR=.
    unzip -o -d $TMP_EXTRACT_DIR $CONFLUENCE_EDITOR_JAR templates/editor-
preload-container.vm;
    if [ ! -f templates/editor-preload-container.vm ]
    then
        echo "ERROR: Failed to extract templates/editor-preload-container.vm
from $CONFLUENCE_EDITOR_JAR"
        echo ""
        echo "UPDATE FAILED, EXITING!"
        exit 1;
    fi

    echo -n "    h. validating file changes for file within updated JAR.. "
    if grep -qi "action.syncRev" $TMP_EXTRACT_DIR/templates/editor-preload-
container.vm
    then
        echo "ERROR: Failed to update $TMP_EXTRACT_DIR/templates/editor-preload-
container.vm"
        echo ""
        echo "UPDATE FAILED, EXITING!"
        exit 1;
    fi
    if ! grep -qi "value=syncRev" $TMP_EXTRACT_DIR/templates/editor-preload-
container.vm
    then
        echo "ERROR: Failed to update $TMP_EXTRACT_DIR/templates/editor-preload-
container.vm"
        echo ""
        echo "UPDATE FAILED, EXITING!"
        exit 1;
    fi
    echo "ok"

```



```

        echo -n "    i. cleaning up temp files.."
        rm -f $TMP_EXTRACT_DIR/templates/editor-preload-container.vm
$TMP_EXTRACT_DIR/templates/editor-preload-container.vm.bak $TMP_EXTRACT_DIR
/templates/editor-preload-container.vm.original;
        rmdir $TMP_EXTRACT_DIR/templates 2> /dev/null;
        echo "ok"
    else
        echo "    b. templates/editor-preload-container.vm not present in JAR,
skipping step"
    fi
else
    echo "    b. JAR not present in current install, skipping step"
fi

echo ""
echo "Update completed!"

```

执行后会进行提示

提示页面的变更内容

File 1: 'confluence/users/user-dark-features.vm':

- a. backing up file.. done
- b. updating file.. done
- c. showing file changes..

70c70

```

<                #tag( "Component" "label='Enable dark feature:'" "name='featureKey'"
"value='$!action.featureKey'" "theme='au'" "template='text.vm'")

```

```

>                #tag( "Component" "label='Enable dark feature:'" "name='featureKey'"
"value=featureKey" "theme='au'" "template='text.vm'")

```

- d. validating file changes.. ok
- e. file updated successfully!

File 2: 'confluence/login.vm':

- a. backing up file.. done
- b. updating file.. done
- c. showing file changes..

169c169

```

<                #tag( "Hidden" "name='token'" "value='$!action.token'" )

```

```

>                #tag( "Hidden" "name='token'" "value=token" )

```

- d. validating file changes.. ok

- e. file updated successfully!

File 3: 'confluence/pages/createpage-entervariables.vm':

- a. backing up file.. done
- b. updating file.. done
- c. showing file changes..

24c24

```
<          #tag ("Hidden" "name='queryString'" "value='$!queryString'")
```

```
>          #tag ("Hidden" "name='queryString'" "value=queryString")
```

26c26

```
<          #tag ("Hidden" "name='linkCreation'" "value='$!linkCreation'")
```

```
>          #tag ("Hidden" "name='linkCreation'" "value=linkCreation")
```

- d. validating file changes..ok
- e. file updated successfully!

File 4: 'confluence/template/custom/content-editor.vm':

- a. backing up file.. done
- b. updating file.. done
- c. showing file changes..

64c64

```
<          #tag ("Hidden" "name='queryString'" "value='$!queryString'")
```

```
>          #tag ("Hidden" "name='queryString'" "value=queryString")
```

85c85

```
<          #tag ("Hidden" "id=sourceTemplateId" "name='sourceTemplateId'"  
"value='$!{templateId}'")
```

```
>          #tag ("Hidden" "id=sourceTemplateId" "name='sourceTemplateId'"  
"value=templateId")
```

- d. file updated successfully!

File 5: 'confluence/WEB-INF/atlassian-bundled-plugins/confluence-editor-loader*.jar':

- a. extracting templates/editor-preload-container.vm from confluence/WEB-INF/atlassian-bundled-plugins/confluence-editor-loader-7.10.2.jar..

Archive: confluence/WEB-INF/atlassian-bundled-plugins/confluence-editor-loader-7.10.2.jar

inflating: ./templates/editor-preload-container.vm

- b. updating file.. done
- c. showing file changes..

56c56

```
< #tag ("Hidden" "id=syncRev" "name='syncRev'" "value='$!{action.syncRev}'")
```

```
> #tag ("Hidden" "id=syncRev" "name='syncRev'" "value=syncRev")
  d. validating file changes.. ok
  e. updating confluence/WEB-INF/atlassian-bundled-plugins/confluence-editor-
loader-7.10.2.jar with ./templates/editor-preload-container.vm..updating: templates
/editor-preload-container.vm (deflated 59%)
-rw-r--r-- 1 root root 13373 Sep  3 05:09 confluence/WEB-INF/atlassian-bundled-
plugins/confluence-editor-loader-7.10.2.jar
  f. cleaning up temp files..ok
  g. extracting templates/editor-preload-container.vm from confluence/WEB-INF
/atlassian-bundled-plugins/confluence-editor-loader-7.10.2.jar again to check
changes within JAR..
Archive:  confluence/WEB-INF/atlassian-bundled-plugins/confluence-editor-loader-
7.10.2.jar
  inflating: ./templates/editor-preload-container.vm
  h. validating file changes for file within updated JAR.. ok
  i. cleaning up temp files..ok
```

Update completed!