긴급패치 CVE-2021-26084 취약성 조치 방법

이 문서는 CVE-2021-26084 취약점에 대한 조치 방법을 공유하기 위해 작성되었다.

영향 받는 제품

- Confluence Server
- Confluence Data Center

보안 패치 방법

긴급 패치 적용 전, Confluence 설치 폴더를 백업하여 문제가 생겼을 시에 해당 파일로 원복한다.

Linux

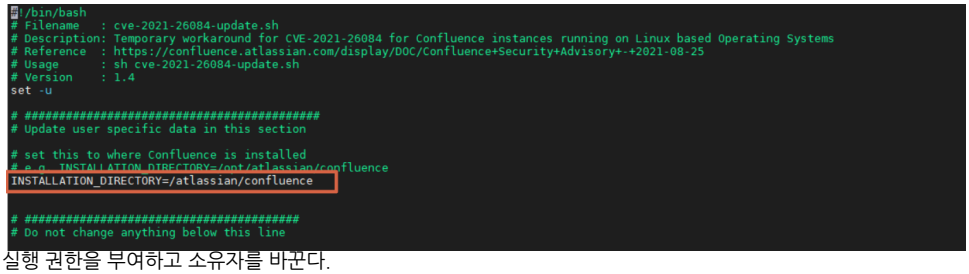
1. Confluence를 종료한다.
2. cve-2021-26084-update.sh 파일을 다운로드 받아 linux 서버로 이동한다. (예시) /home/atlassian)
3. cve-2021-26084-update.sh 파일을 편집한다.

```
<INSTALL_DIRECTORY>      .
```

/home/atlassian

```
vi cve-2021-26084-update.sh


########################################################################
INSTALLATION_DIRECTORY=<  >
```



```
#!/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=/atlassian/confluence

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

4. 실행 권한을 부여하고 소유자를 바꾼다.

```
#
chmod 700 cve-2021-26084-update.sh

# Confluence
$ ls -l /atlassian/confluence-7.4.0 | grep bin
drwxr-xr-x.  3 atlassian atlassian  4096 Jun 28 16:52 bin

# cve-2021-26084-update.sh
chown -R <confluence  >: cve-2021-26084-update.sh
) chown -R atlassian: cve-2021-26084-update.sh


-rwx------  1 atlassian atlassian     10400 Sep  7 08:54 cve-2021-26084-update.sh
```

5. Linux 사용자를 Confluence 설치 디렉토리의 소유자로 바꾼다.

```
#
$ sudo su <confluence  >
) $ sudo su atlassian
```

6. 스크립트를 실행한다.

```
./cve-2021-26084-update.sh
```

7. 업데이트 된 최대 5개의 파일을 확인하고 다음으로 끝나야한다. (업데이트 되는 파일의 수는 Confluence 버전에 따라 다르다.)

```
Update completed!
```

```
chdir '/atlassian/confluence'

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='aui'" "template='text.vm'")
---
>             #tag( "Component" "label='Enable dark feature:'" "name='featureKey'" "value=featureKey"
"theme='aui'" "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..
147c147
<                         #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-7.4.0.jar..
Archive:  confluence/WEB-INF/atlassian-bundled-plugins/confluence-editor-loader-7.4.0.jar
  inflating: ./templates/editor-preload-container.vm
   b. updating file.. done
   c. showing file changes..
   d. validating file changes.. ok
   e. updating confluence/WEB-INF/atlassian-bundled-plugins/confluence-editor-loader-7.4.0.jar with .
/templates/editor-preload-container.vm..updating: templates/editor-preload-container.vm (deflated 59%)
-rw-r--r-- 1 atlassian atlassian 13402 Sep  7 15:40 confluence/WEB-INF/atlassian-bundled-plugins
/confluence-editor-loader-7.4.0.jar
   f. cleaning up temp files..ok
   g. extracting templates/editor-preload-container.vm from confluence/WEB-INF/atlassian-bundled-plugins
/confluence-editor-loader-7.4.0.jar again to check changes within JAR..
Archive:  confluence/WEB-INF/atlassian-bundled-plugins/confluence-editor-loader-7.4.0.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!
```

8. Confluence를 시작한다.

Windows

> 클러스터에서 Confluence를 실행하는 경우 모든 노드에서 이 스크립트를 실행해야 한다.

1. Confluence를 종료한다.
2. cve-2021-26084-update.ps1 파일을 다운로드 받아 Windows 서버로 이동한다.
3. cve-2021-26084-update.ps1 파일을 편집한다.

```
INSTALLATION_DIRECTORY Confluence    .
```

```
$INSTALLATION_DIRECTORY='  '


)$INSTALLATION_DIRECTORY='C:\app\atlassian\confluence'
```

4. **관리자 권한**으로 Windows PowerShell을 실행시킨다.
5. PowerShell의 기본 제한 실행 정책으로 인해 다음 명령을 사용하여 PowerShell을 실행한다.

```
Get-Content <cve-2021-26084-update.ps1   > | powershell.exe -noprofile -


) Get-Content C:\Users\admin\Downloads\cve-2021-26084-update.ps1 | powershell.exe -noprofile -
```

6. 업데이트 된 최대 5개의 파일을 확인하고 오류가 발생하지 않으며, 다음으로 끝나야한다. (업데이트 되는 파일의 수는 Confluence 버전에 따라 다르다.)
(오류는 일반적으로 빨간색으로 표시된다)

```
Update completed!
```