链滴

阿里云 ECS “CVE-2018-18311 8.1 Perl_my_setenv() 函数缓冲区溢出漏洞”导致挂载系统磁盘爆满并告警

作者：zorkelvll
原文链接：https://ld246.com/article/1551182735722
来源网站：链滴
许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

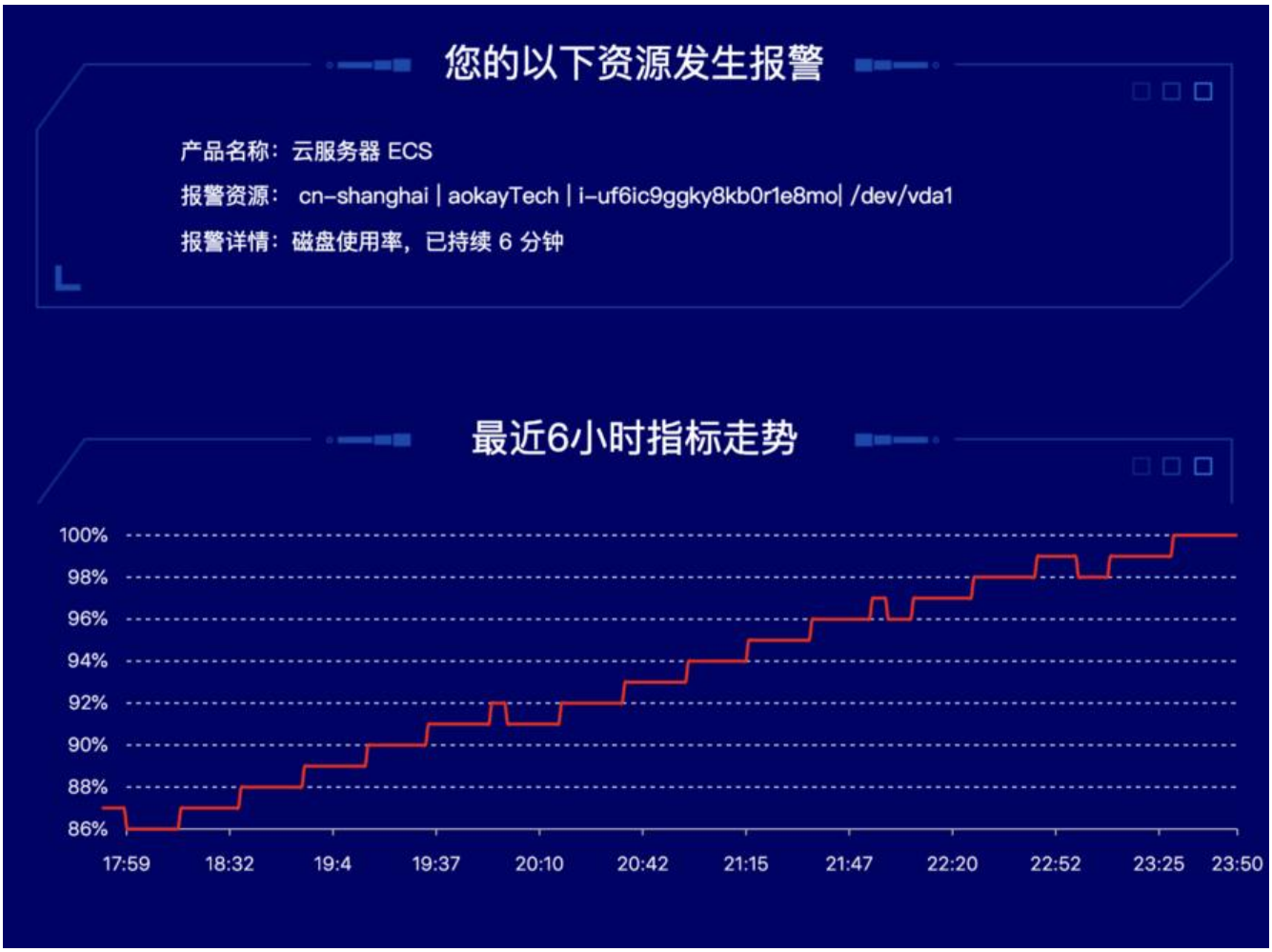
ZERO
    [持续更新](https://zorkelvll.cn/) 请关注：[https://zorkelvll.cn/blog/zorkelvll/articles/2019/02/17/1550418071807](https://zorkelvll.cn/blogs/zorkelvll/articles/209/02/17/1550418071807)

背景

    本文主要是记录阿里云CS主机在遭受perl语言RHSA-2019:0109-Important: perl security update漏洞之后，导致磁盘爆无法写入被告警通知之后的解决步骤策略

一、修复过程

1、2019-02-16 23:51收到阿里云ECS磁盘使用率告警邮件通知



2、登录阿里云控制台发现系统存在漏洞

3、解决办法

原文链接：阿里云 ECS“CVE-2018-18311 8.1 Perl_my_setenv() 函数缓冲区溢出漏洞”导致挂载系统磁盘爆满并告警

yum upgrade perl
yum upgrade perl-ExtUtils-Install
yum upgrade perl-Pod-Escapes
yum update perl-devel
yum upgrade perl-libs
yum upgrade perl-macros

3.1、漏洞修复过程中的问题

在执行3的过程中，由于磁盘已经被占满导致无法安装补丁，进而无法修复漏洞

分析：由于该漏洞是perl语言的，而自己所在服务器中是在jumpserver - coco应用服务中需要perl语支持的，因此有针对性地使用du -sh命令查看各个文件夹的大小尤其是coco相关的文件

```
[[root@aokayTech /]# du -sh opt/
31G     opt/
```

```
[[root@aokayTech opt]# du -sh coco/
30G     coco/
```

```
[(py3) [root@aokayTech coco]# du -sh logs/
30G     logs/
```

```
[(py3) [root@aokayTech logs]# ll -a
总用量 30801496
drwxr-xr-x  2 root root        4096 2月  17 00:21 .
drwxr-xr-x 10 root root        4096 11月 15 20:09 ..
-rw-rw-rw-  1 root root   319512282 2月  17 00:46 coco.log
-rw-rw-rw-  1 root root       59598 2月  10 17:43 coco.log.2019-02-09
-rw-rw-rw-  1 root root      134287 2月  11 18:19 coco.log.2019-02-10
-rw-rw-rw-  1 root root    26684628 2月  12 21:52 coco.log.2019-02-11
-rw-rw-rw-  1 root root      832262 2月  13 21:35 coco.log.2019-02-12
-rw-rw-rw-  1 root root    26318624 2月  14 18:31 coco.log.2019-02-13
-rw-rw-rw-  1 root root  7643216146 2月  16 00:20 coco.log.2019-02-15
-rw-rw-rw-  1 root root 23523911085 2月  17 00:20 coco.log.2019-02-16
```

=》该漏洞导致coco应用的日志剧增，写爆了磁盘！因此，在此处手工清空该日志文件夹，再重新执3中的漏洞修复即可

4、阿里云ECS控制，漏洞管理界面，执行漏洞检测该漏洞，验证确保该漏洞修复成功

状态(全部)	说明		首次/最后发现时间	操作
修复成功	软件: perl 5.16.3-292.el7 命中: perl version less than 4:5.16.3-294.el7_6	更多	2019-02-16 09:15:25 2019-02-16 09:15:25	--

二、总结

1、贫穷的无奈 - 因穷，无法购买阿里云企业版的一些服务，则只能自己手动修复漏洞

2、迟来的告警 - 漏洞出现许久之后，因漏洞而导致的磁盘爆满之后的磁盘告警，而非漏洞修复邮件醒

3、自身的响应解决漏洞的效率不够及时，直接就慌张了 - 差一点执行了最愚蠢最无能的将机器重置操作了

4、服务器中的各项应用服务，没有均保证是开机自启，且没有一个统一的脚本去处理运行的服务