Huawei Cloud EulerOS

服务公告

文档版本	01
发布日期	2026-08-04

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 漏洞公告.....1
1.1 OpenSSH 远程代码执行漏洞公告（CVE-2024-6387）.....1
1.2 Linux Kernel 本地权限提升漏洞"Copy Fail"（CVE-2026-31431）.....2
1.3 Linux Kernel 本地权限提升漏洞"Dirty Frag"（CVE-2026-43284）.....6

1 漏洞公告

1.1 OpenSSH远程代码执行漏洞公告（CVE-2024-6387）
1.2 Linux Kernel本地权限提升漏洞"Copy Fail"（CVE-2026-31431）
1.3 Linux Kernel本地权限提升漏洞"Dirty Frag"（CVE-2026-43284）

1.1 OpenSSH 远程代码执行漏洞公告（CVE-2024-6387）

漏洞详情

2024年7月1日，国外安全研究机构发布了最新的一个关于“regreSSHion: RCE in OpenSSH's server, on glibc-based Linux systems(CVE-2024-6387)” 的漏洞公告，该漏洞影响的HCE OpenSSH版本范围：8.5p1 <= OpenSSH < 8.8p1-2.r34。由于sshd在SIGALRM处理程序中调用了不安全的异步信号函数，导致未经身份验证的攻击者利用漏洞可以在受害者Linux系统上以root身份执行任意代码。该漏洞影响范围广，目前漏洞技术细节和PoC均已公开，建议用户及时修复。

HCE对应的SA参见：**HCE2-SA-2024-0224**。

影响和风险

未经身份验证的攻击者可以利用此漏洞在Linux系统上以root身份执行任意代码，造成机密性、完整性和可用性全面损失。

判断方法

1. 执行以下命令查看HCE版本，如果显示hceversion=HCE-2.0.xxxx，执行下一步；如果是hceversion=HCE-1.1.xxxx，则不受该漏洞影响。
   ```
   cat /etc/hce-latest
   ```
2. 执行以下命令查询OpenSSH版本号，如果版本号小于8.8p1-2.r34，说明受该漏洞影响。
   ```
   rpm -q openssh
   ```

漏洞修复方案

1. 升级OpenSSH版本。
   ```
   yum update -y openssh
   ```


2. 查询OpenSSH版本号，如果版本号大于等于8.8p1-2.r34，表示OpenSSH版本已更新。
```
rpm -q openssh
```
3. 重启sshd服务。
```
systemctl restart sshd
```

参考链接

https://nvd.nist.gov/vuln/detail/CVE-2024-6387

https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt

1.2 Linux Kernel 本地权限提升漏洞"Copy Fail"（CVE-2026-31431）

漏洞详情

2026年4月30日，安全研究团队公开披露了一个存在于 Linux Kernel 的高危本地权限提升漏洞 "Copy Fail"（CVE-2026-31431）。该漏洞影响自2017年以来所有主流Linux发行版(kernel >= 4.14)，攻击者仅凭一个732字节的Python脚本即可从普通用户权限直接提升至root权限，并可能导致容器逃逸、云环境租户隔离被突破等严重后果。该漏洞影响范围广，目前漏洞技术细节和PoC均已公开，建议用户及时修复。

HCE对应的SA参见：

HCE 2.0 Security Advisories

HCE 3.0 Security Advisories

影响和风险

普通用户可以利用此漏洞在Linux系统上执行一个732字节的Python脚本即可从普通用户权限直接提升至root权限，容器场景可以从容器内实现逃逸，造成机密性、完整性和可用性全面损失。

判断方法

1. 执行以下命令查看HCE版本，如果有回显，执行下一步；如果没有回显，则非HCE版本或者不受该漏洞影响。
```
# cat /etc/hce-latest | grep -E "HCE-2.0|HCE-3.0"
```
2. 执行以下命令查询kernel版本号。

   如果是5.10内核，检查版本号是否>=5.10.0-182.0.0.95.r3450_281.hce2，“是”则说明不受该漏洞影响，否则受影响。

   如果是6.6内核，检查版本号是否>=6.6.0-72.0.0.76.r1245_84.hce3，“是”则说明不受该漏洞影响，否则受影响。
```
# uname -r
```

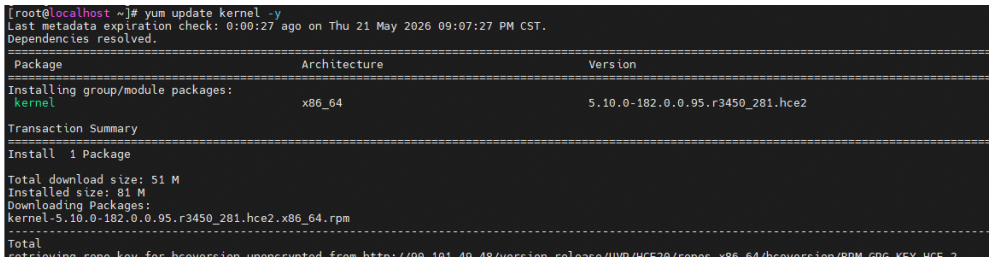
漏洞修复方案

须知

当前只有部分内核版本支持升级热补丁修复，热补丁支持内核版本基线列表请参考：**表1 热补丁支持内核版本基线列表**。

对于不在支持范围内的内核版本，建议先将kernel升级支持范围内，再打热补丁，或者直接升级冷补丁包。

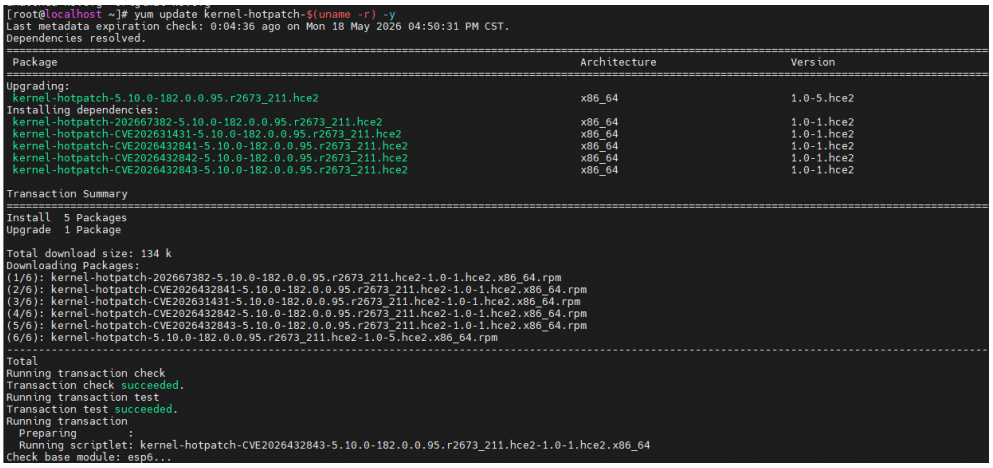
方案一：升级冷补丁

1. 升级kernel版本。
   ```
   # yum update kernel -y
   ```
   
   ```
   [root@localhost ~]# yum update kernel -y
   Last metadata expiration check: 0:00:27 ago on Thu 21 May 2026 09:07:27 PM CST.
   Dependencies resolved.
   ================================================================================
    Package                 Architecture                 Version
   ================================================================================
   Installing group/module packages:
    kernel                  x86_64                       5.10.0-182.0.0.95.r3450_281.hce2

   Transaction Summary
   ================================================================================
   Install  1 Package

   Total download size: 51 M
   Installed size: 81 M
   Downloading Packages:
   kernel-5.10.0-182.0.0.95.r3450_281.hce2.x86_64.rpm
   --------------------------------------------------------------------------------
   Total
   ```
2. 重启系统生效。
   ```
   # reboot
   ```
3. 重启登录系统后，执行以下命令查询当前内核版本号。
   ```
   # uname -r
   ```
   如果是5.10内核，检查版本号是否>=5.10.0-182.0.0.95.r3450_281.hce2，“是”则说明该漏洞已修复，不受影响。

   如果是6.6内核，检查版本号是否>=6.6.0-72.0.0.76.r1245_84.hce3，“是”则说明该漏洞已修复，不受影响。

方案二：升级热补丁

1. 安装热补丁前，先升级或安装kpatch-runtime包，执行以下命令检查环境是否安装kpatch-runtime包。
   ```
   # rpm -qa | grep kpatch-runtime
   ```
   如果没有安装，执行以下命令进行安装。
   ```
   # yum install kpatch-runtime -y
   ```
   如果已经安装，需执行以下命令进行升级。
   ```
   # yum update kpatch-runtime -y
   ```
2. 执行以下命令设置升级的内核热补丁版本。
   ```
   # grep -q "HCE-2.0" /etc/hce-latest && kernel_hot_version="1.0-5.hce2" ||
   kernel_hot_version="1.0-2.hce3"
   ```
3. 执行以下命令升检查环境是否安装kernel-hotpatch包。
   ```
   # rpm -qa | grep kernel-hotpatch
   ```
   如果没有回显，表示没有安装，执行以下命令进行安装。
   ```
   # yum install kernel-hotpatch-$(uname -r | sed 's/\.\(x86_64\|aarch64\)$//')-$kernel_hot_version -y
   ```
   如果有回显，表示已经安装，需执行以下命令进行升级。
   ```
   # yum update kernel-hotpatch-$(uname -r | sed 's/\.\(x86_64\|aarch64\)$//')-$kernel_hot_version -y
   ```



4. 执行以下命令确认热补丁名称为：Patch Name: CVE202631431，补丁状态为：Patch State: Active。

```
# livepatch -q | grep "Patch Name: CVE202631431" -A 13
```

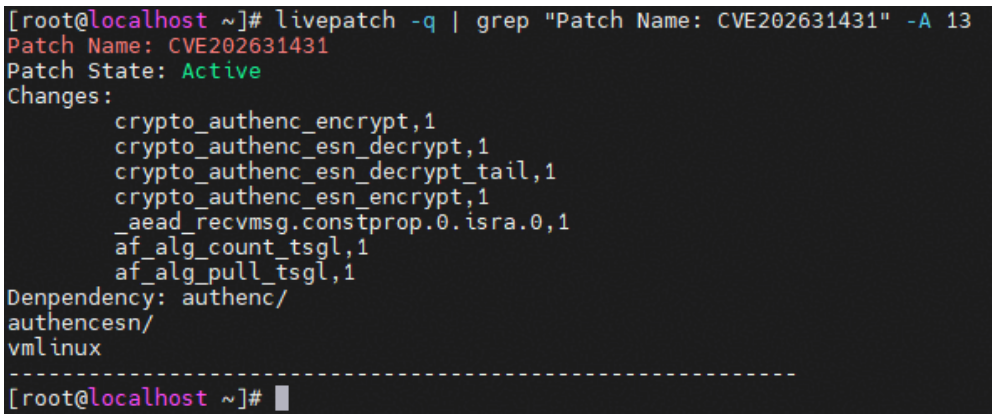


表 1-1 热补丁支持内核版本基线列表

HCE版本	内核版本
HCE-2.0	5.10.0-182.0.0.95.r2453_180.hce2
	5.10.0-182.0.0.95.r2572_186.hce2
	5.10.0-182.0.0.95.r2673_211.hce2
	5.10.0-182.0.0.95.r2762_220.hce2
	5.10.0-182.0.0.95.r2825_235.hce2
	5.10.0-182.0.0.95.r2947_236.hce2
	5.10.0-182.0.0.95.r3008_246.hce2
	5.10.0-182.0.0.95.r3090_252.hce2
	5.10.0-182.0.0.95.r3184_259.hce2
	5.10.0-182.0.0.95.r3304_260.hce2
	5.10.0-182.0.0.95.r3353_273.hce2

HCE版本	内核版本
HCE-3.0	6.6.0-72.0.0.76.r1014_62.hce3
	6.6.0-72.0.0.76.r1152_80.hce3

⚠ 注意

如果环境实施过规避措施（禁用authenc和authencesn模块），需先回退规避措施，再升级热补丁，否则会导致热补丁升级失败，补丁不生效。（热补丁修改内容依赖authenc和authencesn模块加载，规避措施和升级热补丁是冲突的）。

补丁回退方案

如果执行漏洞修复后，发生不可预期结果，需要回退修复补丁，可执行以下操作：

步骤1 执行以下查询升级补丁操作的ID，如下图升级补丁的ID为3。

```
# yum history
```

```
[root@localhost ~]# yum history
ID     | Command line
-------------------------------------------------------------------------------
     3 | update kernel-hotpatch-5.10.0-182.0.0.95.r2673_211.hce2.x86_64 -y
     2 | install kpatch-runtime
     1 |
```

步骤2 使用 **1** 中查询到ID，执行以下命令进行回退。

```
# yum history undo 【ID】
```

```
[root@localhost ~]# yum history undo 3
Last metadata expiration check: 0:00:34 ago on Mon 15 Jun 2026 11:53:11 AM CST.
Dependencies resolved.
================================================================================
 Package                                    Architecture                  Ver
================================================================================
Removing dependent packages:
 kernel-hotpatch-202667382-5.10.0-182.0.0.95.r2673_211.hce2                x86_64                        1.0
 kernel-hotpatch-CVE202631431-5.10.0-182.0.0.95.r2673_211.hce2             x86_64                        1.0
 kernel-hotpatch-CVE2026432841-5.10.0-182.0.0.95.r2673_211.hce2            x86_64                        1.0
 kernel-hotpatch-CVE2026432842-5.10.0-182.0.0.95.r2673_211.hce2            x86_64                        1.0
 kernel-hotpatch-CVE2026432843-5.10.0-182.0.0.95.r2673_211.hce2            x86_64                        1.0
Downgrading:
 kernel-hotpatch-5.10.0-182.0.0.95.r2673_211.hce2                          x86_64                        1.0

Transaction Summary
================================================================================
Remove     5 Packages
Downgrade  1 Package

Total download size: 3.2 k
Is this ok [y/N]: y
Downloading Packages:
kernel-hotpatch-5.10.0-182.0.0.95.r2673_211.hce2-1.0-0.hce2.x86_64.rpm
--------------------------------------------------------------------------------
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
  Downgrading      : kernel-hotpatch-5.10.0-182.0.0.95.r2673_211.hce2-1.0-0.hce2.x86_64
  Cleanup          : kernel-hotpatch-5.10.0-182.0.0.95.r2673_211.hce2-1.0-5.hce2.x86_64
  Running scriptlet: kernel-hotpatch-202667382-5.10.0-182.0.0.95.r2673_211.hce2-1.0-1.hce2.x86_64
disabling patch module: klp_202667382
unloading patch module: klp_202667382

  Erasing          : kernel-hotpatch-202667382-5.10.0-182.0.0.95.r2673_211.hce2-1.0-1.hce2.x86_64
  Running scriptlet: kernel-hotpatch-202667382-5.10.0-182.0.0.95.r2673_211.hce2-1.0-1.hce2.x86_64
  Running scriptlet: kernel-hotpatch-CVE202631431-5.10.0-182.0.0.95.r2673_211.hce2-1.0-1.hce2.x86_64
disabling patch module: klp_CVE202631431
unloading patch module: klp_CVE202631431
uninstalling klp_CVE202631431.ko (5.10.0-182.0.0.95.r2673_211.hce2.x86_64)

  Erasing          : kernel-hotpatch-CVE202631431-5.10.0-182.0.0.95.r2673_211.hce2-1.0-1.hce2.x86_64
  Running scriptlet: kernel-hotpatch-CVE202631431-5.10.0-182.0.0.95.r2673_211.hce2-1.0-1.hce2.x86_64
  Running scriptlet: kernel-hotpatch-CVE2026432841-5.10.0-182.0.0.95.r2673_211.hce2-1.0-1.hce2.x86_64
```

----结束

规避方案

如果暂时无法升级修复补丁，建议先禁用authenc和authencesn模块实施规避。

步骤1 执行以下命令检查禁用模块authenc和authencesn是否加载，如果有回显，说明模块有加载，执行**2**；如果没有回显，执行**3**。

```
# lsmod | grep -E "authenc|authencesn"
```

步骤2 如果authenc或authencesn模块加载了，需客户自行排查是否有业务在使用，如果没有，可执行以下命令卸载，然后执行**3**；如果有，建议参考**方案一**或者**方案二**进行补丁升级，尽快修复漏洞。

```
# modprobe -r authencesn
# modprobe -r authenc
```

步骤3 执行以下命令 ，禁止authenc和authencesn模块加载。执行后即时生效，无需重启系统。

```
# echo "install authenc /bin/false" >> /etc/modprobe.d/blacklist.conf
# echo "install authencesn /bin/false" >> /etc/modprobe.d/blacklist.conf
```

----结束

参考链接

https://nvd.nist.gov/vuln/detail/CVE-2026-31431

https://copy.fail

1.3 Linux Kernel 本地权限提升漏洞"Dirty Frag"（CVE-2026-43284）

漏洞详情

2026年5月8日，业界公开了一个 Linux 内核高危本地权限提升（LPE）漏洞。它是继不久前的 Copy Fail (CVE-2026-31431) 之后，又一个利用内核页面缓存（Page Cache）实现提权的逻辑漏洞，该漏洞被命名为Dirty Frag。通过同时利用 xfrm-ESP Page-Cache Write 和 RxRPC Page-Cache Write 两个逻辑缺陷，实现对 struct sk_buff 中 frag 成员的定向污染，从而向任意可读文件的 page cache 执行确定性写入。该漏洞影响所有主流Linux发行版(kernel >= 4.11)，攻击者已公开PoC程序即可从普通用户权限直接提升至root权限。其中，HCE受影响是xfrm-esp（CVE-2026-43284），不受rxrpc（cve-2026-43500）影响。该漏洞影响范围广，目前漏洞技术细节和PoC均已公开，建议用户及时修复。

HCE对应的SA参见：

HCE 2.0 Security Advisories

HCE 3.0 Security Advisories

影响和风险

普通用户可以利用此漏洞在Linux系统上从普通用户权限直接提升至root权限，造成机密性、完整性和可用性全面损失。

判断方法

1. 执行以下命令查看HCE版本，如果有回显，执行下一步；如果没有回显，则非HCE版本或者不受该漏洞影响。
```
# cat /etc/hce-latest | grep -E "HCE-2.0|HCE-3.0"
```
2. 执行以下命令查询kernel版本号。

   如果是5.10内核，检查版本号是否>=5.10.0-182.0.0.95.r3450_281.hce2，“是”则说明不受该漏洞影响，否则受影响。

   如果是6.6内核，检查版本号是否>=6.6.0-72.0.0.76.r1245_84.hce3，“是”则说明不受该漏洞影响，否则受影响。
```
# uname -r
```

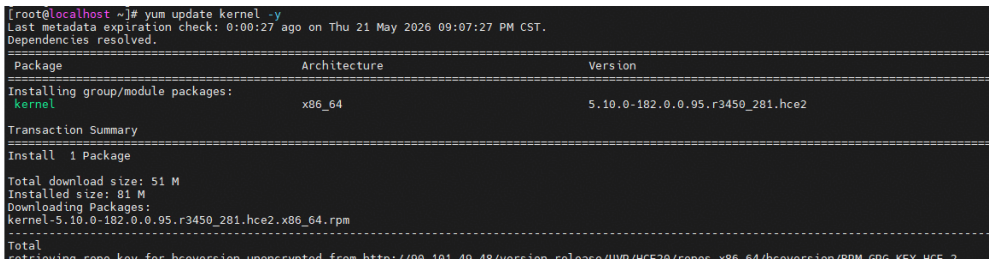
漏洞修复方案

须知

当前只有部分内核版本支持升级热补丁修复，热补丁支持的内核版本基线列表请参考：**表1 热补丁支持的内核版本基线列表**。

对于不在支持范围内的内核版本，建议先将kernel升级支持范围内，再打热补丁，或者直接升级冷补丁包。

方案一：升级冷补丁

1. 升级kernel版本。
```
# yum update kernel -y
```


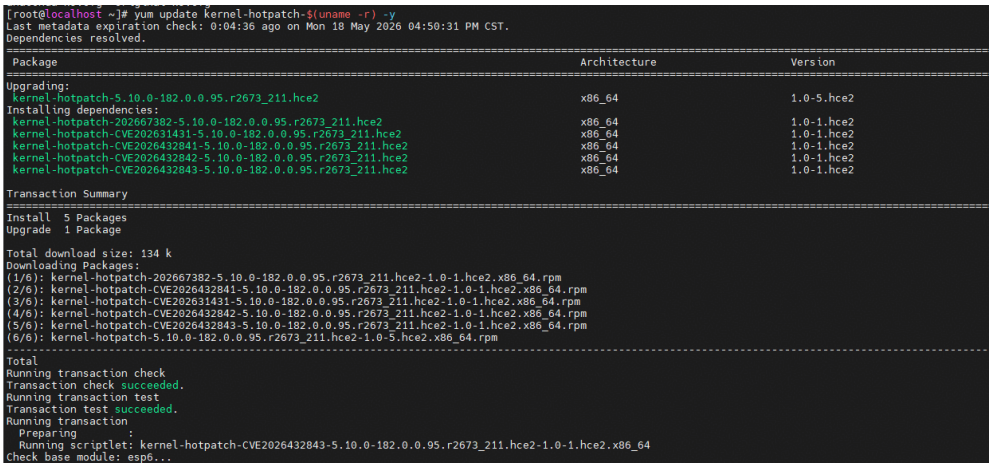
2. 重启系统生效。
```
# reboot
```
3. 重启登录系统后，执行以下命令查询当前内核版本号。
```
# uname -r
```
   如果是5.10内核，检查版本号是否>=5.10.0-182.0.0.95.r3450_281.hce2，“是”则说明该漏洞已修复，不受影响。

   如果是6.6内核，检查版本号是否>=6.6.0-72.0.0.76.r1245_84.hce3，“是”则说明该漏洞已修复，不受影响。

方案二：升级热补丁

1. 安装热补丁前，先升级或安装kpatch-runtime包，执行以下命令检查环境是否安装kpatch-runtime包。
```
# rpm -qa | grep kpatch-runtime
```
   如果搜索不到，执行以下命令进行安装。
```
# yum install kpatch-runtime -y
```
   如果搜索有结果，执行以下命令进行升级。
```
# yum update kpatch-runtime -y
```

2. 执行以下命令设置升级的内核热补丁版。
```
# grep -q "HCE-2.0" /etc/hce-latest && kernel_hot_version="1.0-5.hce2" ||
kernel_hot_version="1.0-2.hce3"
```
3. 执行以下命令升检查环境是否安装kernel-hotpatch包。
```
# rpm -qa | grep kernel-hotpatch
```
如果没有回显，表示没有安装，执行以下命令进行安装。
```
# yum install kernel-hotpatch-$(uname -r | sed 's/\.\(x86_64\|aarch64\)$//')-$kernel_hot_version -y
```
如果有回显，表示已经安装，需执行以下命令进行升级。
```
# yum update kernel-hotpatch-$(uname -r | sed 's/\.\(x86_64\|aarch64\)$//')-$kernel_hot_version -y
```



4. 执行以下命令确认热补丁名称为：Patch Name: CVE2026432842，补丁状态为：Patch State: Active。
```
# livepatch -q | grep "Patch Name: CVE202643284*" -A 6
```

表 1-2 热补丁支持的内核版本基线列表

HCE版本	内核版本
HCE-2.0	5.10.0-182.0.0.95.r2453_180.hce2
	5.10.0-182.0.0.95.r2572_186.hce2
	5.10.0-182.0.0.95.r2673_211.hce2
	5.10.0-182.0.0.95.r2762_220.hce2
	5.10.0-182.0.0.95.r2825_235.hce2
	5.10.0-182.0.0.95.r2947_236.hce2
	5.10.0-182.0.0.95.r3008_246.hce2
	5.10.0-182.0.0.95.r3090_252.hce2
	5.10.0-182.0.0.95.r3184_259.hce2

HCE版本	内核版本
	5.10.0-182.0.0.95.r3304_260.hce2
	5.10.0-182.0.0.95.r3353_273.hce2
HCE-3.0	6.6.0-72.0.0.76.r1014_62.hce3
	6.6.0-72.0.0.76.r1152_80.hce3

⚠ 注意

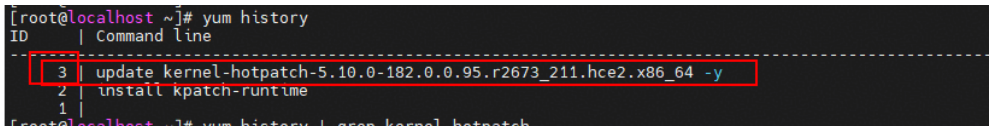
如果环境实施过规避措施（禁用esp4和esp6模块），需先回退规避措施，再升级热补丁，否则会导致补丁不生效。（热补丁修改内容依赖esp4和esp6模块加载，规避措施和升级热补丁是冲突的）。

补丁回退方案

如果执行漏洞修复后，发生不可预期结果，需要回退修复补丁，可执行以下操作：

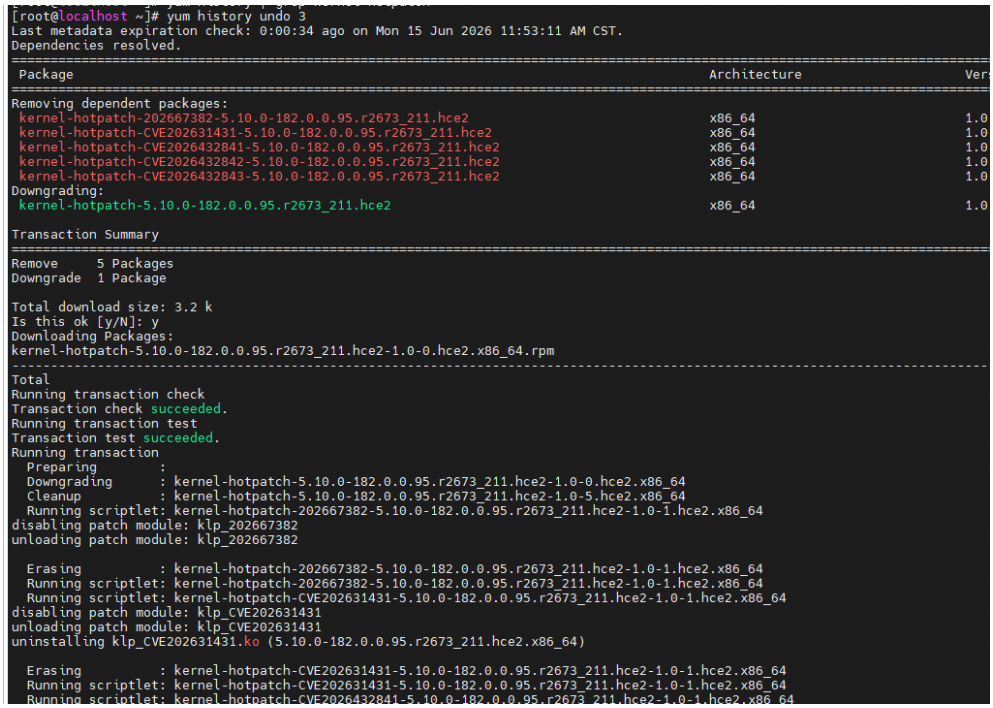
步骤1 执行以下查询升级补丁操作的ID，如下图升级补丁的ID为3。

```
# yum history
```



步骤2 使用 **1** 中查询到ID，执行以下命令进行回退。

```
# yum history undo【ID】
```

----结束

规避方案

如果暂时无法升级修复补丁，建议先禁用esp4和esp6模块实施规避。

步骤1 执行以下命令检查禁用模块esp4和esp6是否加载，如果有回显，说明模块有加载，执行**2**；如果没有回显，执行**3**。

```
# lsmod | grep -E "esp4|esp6"
```

步骤2 如果esp4或esp6模块加载了，需客户自行排查是否有业务在使用，如果没有，可执行以下命令卸载，然后执行**3**；如果有，建议参考**方案一**或者**方案二**进行补丁升级，尽快修复漏洞。

```
# modprobe -r esp4
# modprobe -r esp6
```

步骤3 执行以下命令 ，禁止esp4和esp6模块加载。执行后即时生效，无需重启系统。

```
# echo "install esp4 /bin/false" >> /etc/modprobe.d/disable-esp.conf
# echo "install esp6 /bin/false" >> /etc/modprobe.d/disable-esp.conf
```

----结束

参考链接

https://nvd.nist.gov/vuln/detail/CVE-2026-43284