Huawei Cloud EulerOS

服务公告

文档版本 01

发布日期 2024-07-05

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 漏洞公告

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，如果是HCE 2.0，执行下一步；如果是HCE 1.1，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openssh-8.8p1-2.r34，说明受该漏洞影响。
   ```
   rpm -qa | grep openssh
   ```

漏洞修复方案

1. 升级OpenSSH版本
   ```
   yum update openssh
   ```
   查询OpenSSH版本号是否大于等于openssh-8.8p1-2.r34
   ```
   rpm -qa | grep openssh
   ```
2. 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