Huawei Cloud EulerOS

Product Bulletin

Issue	01
Date	2024-07-05

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Vulnerability Notice

1.1 CVE-2024-6387: OpenSSH Remote Code Execution Vulnerability

Description

On July 1, 2024, a security research institute outside China released the latest vulnerability notice on regreSSHion: RCE in OpenSSH's server, on glibc-based Linux systems (CVE-2024-6387). This vulnerability affects OpenSSH with a version of 8.5p1 or later but earlier than 8.8p1-2.r34. sshd invokes insecure asynchronous signal functions in the SIGALRM signal. As a result, an unauthenticated attacker can exploit this vulnerability to execute arbitrary code as user **root** on the victim's Linux system. This vulnerability has a wide impact. The technical details and PoC of this vulnerability have been disclosed. You are advised to fix the vulnerability in a timely manner.

For details about the HCE SA, see **HCE2-SA-2024-0224**.

Impacts and Risks

Unauthenticated attackers can exploit this vulnerability to execute arbitrary code as user **root** on the Linux system, causing confidentiality, integrity, and availability damage.

Identification Method

1. Check the HCE OS version. If the version is HCE 2.0, go to the next step. If the version is HCE 1.1, the system is not affected by the vulnerability.
   ```
   cat /etc/hce-latest
   ```
2. Check the OpenSSH version. If the version is earlier than 8.8p1-2.r34, the OpenSSH is affected by the vulnerability.
   ```
   rpm -qa | grep openssh
   ```

Solution

1. Upgrade the OpenSSH version.


```
yum update openssh
```

Verify that the OpenSSH version is 8.8p1-2.r34 or later.

```
rpm -qa | grep openssh
```

2. Restart the sshd service.

```
systemctl restart sshd
```

Reference

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

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

