OpenSSH Remote Code Execution Vulnerability (CVE-2024-6387) Risk Alert

Antiy CERT

First published time: July 2, 2024

The original report is in Chinese, and this version is an AI-translated edition.

1 Vulnerability Description

OpenSSH is a set of secure network utilities based on the Secure Shell (SSH) protocol, which provides encryption to protect privacy and secure file transfers, making it the tool of choice for remote server management and secure data communications.

Recently, Antiy CERT has discovered that OpenSSH has fixed a remote code execution vulnerability (CVE-2024-6387). The vulnerability is caused by a signal handler race in the OpenSSH server (sshd). Unauthenticated attackers can exploit this vulnerability to execute arbitrary code as root on Linux systems. Currently, the technical details of the vulnerability (including PoC) have been made public on the Internet. There are nearly 10 million OpenSSH instances publicly available on the Internet. It is recommended that users affected by the vulnerability upgrade to the latest version to fix the vulnerability in a timely manner, or adopt security measures to strengthen protection capabilities and prevent network attacks.

2 Impact Scope

- OpenSSH < 4.4p1
- 8.5p1 <= OpenSSH < 9.8p1

3 Preliminary Vulnerability Analysis

Based on information from all parties and preliminary verification results, Antiy CERT believes that a lthough it takes 6 to 8 hours for an attacker to successfully attack in an environment with address distrib ution randomization (ASLR) enabled based on the publicly available PoC, and there may be consequences of memory corruption, it cannot be concluded that this is a vulnerability that is difficult to be effective. The value of the defense time window is only effective for assets with effective protection management, and it is still a great challenge to quickly implement hardening configurations and fix vulnerabilities. Since attackers have the initiative to select targets and attack time windows, and have a large number of zombie/springboard node resources, they can "fish" for breakthrough nodes that lack effective protection management based on a large number of long-term concurrent connections. For defenders without continuous monitoring and response mechanisms and assets without security management and operation mechanisms, their assets and services are often presented as exposed surfaces and attackable surfaces over the years, and the defense value brought by the 6-8 hour operation time window is almost negligible.

Antiy CERT believes that the attack may be used to expand botnets, mine cryptocurrencies and other attack activities, and may also be used by APT attackers to penetrate defenses and move laterally within unmanaged target networks.

At the same time, we also need to be alert to the evolution of vulnerability availability, including the possibility of other combined exploits, including whether the vulnerability exploit itself has some advanced form.

From the perspective of security management and monitoring, it is certain that there will be an increase in traffic connections of related port services in the near future. We should monitor related traffic and connections, pay attention to memory crash events and logs, and take measures such as closing related port services that do not need to be open (default 22), jointly blocking suspicious access IPs, resetting connections that take too long at a time, and setting access IP or range restrictions for device or server management to provide protection.

4 Vulnerability Fix Recommendations

1) Official Fix Recommendations

The official website has released the latest security version to fix this vulnerability. Affected users are advised to upgrade to the following security version.

OpenSSH > 9.8p1

Official website address : https://www.openssh.com/releasenotes.html

2) Vulnerability Mitigation Measures

If the issue cannot be fixed with a patch, the following methods can be used for mitigation.

- Check and enable hardening measures: Ensure that Address Space Layout Randomization (ASLR) is enabled.
- Set user access policies to grant SSH login permissions only to trusted users.
- Enable two-factor authentication (2FA) for the system or host.

LoginGraceTime to 0 in the configuration file to mitigate the RCE risk, but this method is prone to denial of service attacks on sshd, and the defender needs to decide based on his own scenario conditions. Enabling this method will increase the server's connection usage, and it is used in low-frequency dedicate d service scenarios such as host management, device management, and service management, especially for preventing lateral movement of intranet nodes. However, for services that rely on OpenSSH support and a re open, it is necessary to carefully consider whether to adopt this method.

Appendix 1: References

[1]. regreSSHion: Remote Unauthenticated Code Execution Vulnerability in OpenSSH server

https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regression-remote-unauthenticated-code-execution-vulnerability-in-openssh-server

[2]. cve-2024-6387-poc

https://github.com/getdrive/CVE-2024-6387-PoC

Appendix 2: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.