FAQ About OpenSSH

Antiy CERT

First published: July 8, 2024

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

1 What Is OpenSSH? Is It Widely Distributed?

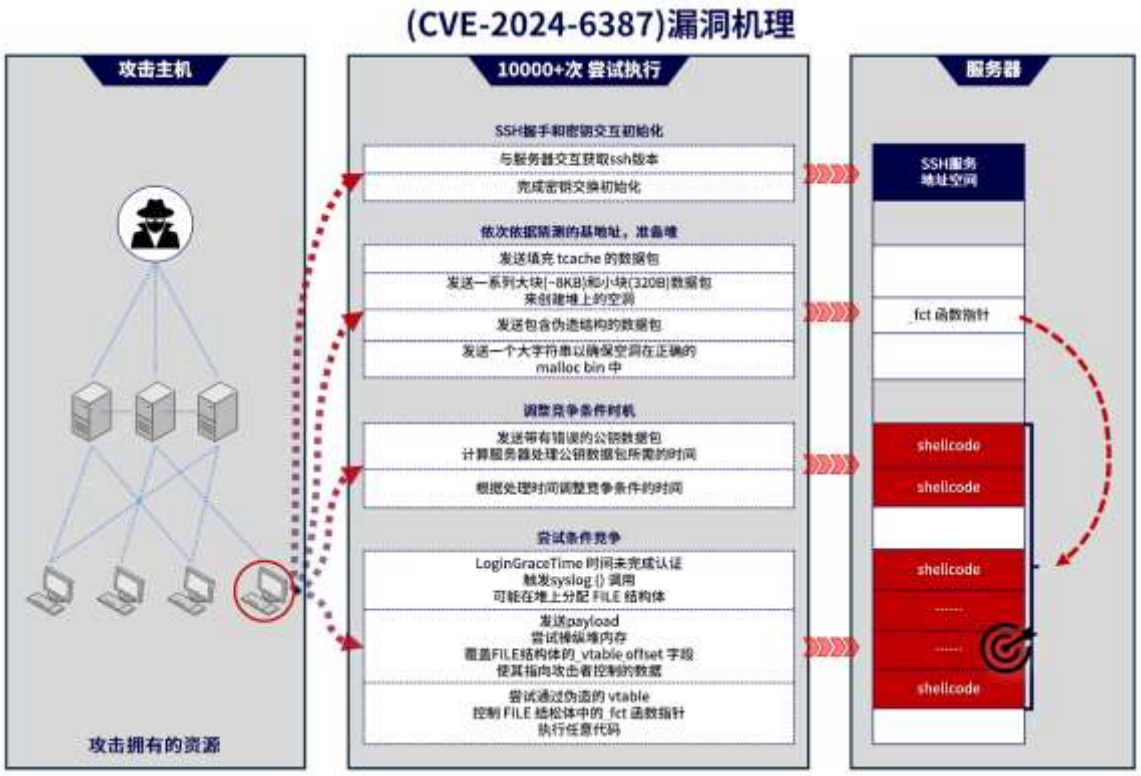
SSH (Secure Shell) is a secure network protocol used to securely transmit data between two untrusted hosts over an insecure network. OpenSSH is an open source implementation of the SSH (Secure Shell) protocol. OpenSSH provides server and client functions and is often used to implement remote login and management (such as remote command execution through the SSH protocol), file transfer (through the SCP or SFTP protocol), and port forwarding. OpenSSH is included in most Linux distributions, macOS, and Windows 10 (through Windows Subsystem for Linux or third-party software).

OpenSSH is widely used in various scenarios with Linux as the underlying system, such as host systems, including servers, cloud hosts, virtual hosts, and some terminals; network devices, including switches, routers, etc.; network security devices, including firewalls, IDS, and other security devices, as well as various security management platforms. Various embedded devices, such as cameras, various IoT devices, etc. Smart home appliances, such as smart TVs, smart refrigerators, and sweeping robots.

2 What Is the Mechanism of the CVE-2024-6387 Vulnerability?

CVE-2024-6387, also known as the regretSSHion vulnerability (CVE-2024-6387), is based on a signal handler race condition when the OpenSSH server (sshd) handles client login timeouts. When the client fails to complete authentication within the time set by LoginGraceTime, sshd triggers the SIGALRM signal handler to execute asynchronously and call the non-asynchronous signal-safe syslog() function, which may perform unsafe memory operations such as malloc() and free(). Attackers take advantage of this opportunity to send specially constructed packets and try to accurately trigger other memory operations during the syslog() call, causing a race condition, which may manipulate heap memory and overwrite critical control data, causing sshd to execute

arbitrary code injected by the attacker after the signal handler ends, achieving unauthorized remote code execution.



To exploit this vulnerability, an attacker needs to make about 10,000 attempts on average, and the target system must be based on a Linux version that uses the GNU C Library (glibc), such as a Debian variant. In addition, the attacker needs to prepare memory structures tailored to a specific version of glibc and Linux. The researchers reproduced the attack on a 32-bit Linux system, but in theory it should also be exploitable on 64-bit systems - albeit with a lower success rate. Address space layout randomization (ASLR) slows down the exploitation process, but does not provide complete protection.

The origin of the regreSSHion vulnerability (CVE-2024-6387) can be traced back to a signal handler race condition in the OpenSSH server (sshd). The issue was originally reported as CVE-2006-5051 as a denial of service (DoS) vulnerability in 2006, and it involved OpenSSH's signal handler calling a function that was not async-signal-safe. Although the original issue was fixed in later versions, in October 2020, due to a code commit (commit 752250c) in OpenSSH version 8.5p1, a change that modified the logging infrastructure accidentally removed a critical protection macro #ifdef DO_LOG_SAFE_IN_SIGHAND, thereby accidentally reintroducing the race condition.

This change caused the originally safe exit call in OpenSSH's sigdie function to be incorrectly changed, thus reintroducing non-async signal safe behavior. Specifically, when sshd's SIGALRM signal handler is triggered, it will

call the syslog() function to record log information, but the call to syslog() in the signal handler is dangerous, it may allocate or release memory in an unsafe context, which may cause heap corruption.

3 Is It Likely That the Vulnerability Will Be Exploited?

Some people believe that the above technical complexity makes large-scale exploitation impractical. Using standard OpenSSH settings to make 10,000 authentication attempts per server takes 6 to 8 hours. In addition, you need to know which version of Linux the server is running. If the server has any protection against brute force cracking and DDoS, these measures may prevent the attack. Therefore, large-scale practical exploitation is unlikely.

Antiy believes that: Although it takes an average of 6 to 8 hours to attack successfully in an environment with address randomization (ASLR) enabled based on the public PoC, and may be accompanied by 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 reinforcement configuration and fix vulnerabilities. Since attackers have the initiative to choose 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 probing of multi-point connections. For these assets without defense management, the defense value brought by the average 6 to 8-hour attack operation time window is almost negligible. It is particularly worth noting that in some device scenarios, in order to save computing resources, ASLR is often turned off, resulting in attacks that can be effective quickly.

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.

4 Which Versions of OpenSSH Are Affected by This Vulnerability?

Currently, the OpenSSH versions known to be affected by this vulnerability are:

- OpenSSH version < 4.4p1

- 8.5p1 <= OpenSSH version < 9.8p1

Other versions are not affected by this vulnerability.

5 How to Fix This Vulnerability?

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

6 What Are the Mitigation Measures When Vulnerabilities Cannot Be Fixed?

If the problem cannot be fixed with a patch, you can use the following methods to mitigate it based on your own scenario.

- 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.

Currently, there is a suggestion to set 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 dedicated 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, it is necessary to carefully consider whether to adopt this method.

7 How Do Antiy's Products Help Users Improve Vulnerabilities?

Currently, many security products of Antiy have the ability to detect and defend against this vulnerability. We strongly recommend that you update the corresponding security products in a timely manner and use security products to check and defend against OpenSSH used in your business.

Antiy Products	Detection and Protection Capabilities
Antiy Unified Workload Protect (UWP)	Product function: Distributed deployment on cloud physical hosts and containers to achieve unified workload protection. UWP can discover components with vulnerabilities, perceive and block attack connections. Upgrade: The vulnerability rule base has been upgraded to version 2024070401, which can discover related vulnerabilities and detect and defend against attacks that exploit the vulnerabilities.
Antiy Persistent Threat Detection System (PTD)	Product function: Deployed at key network nodes to detect network traffic and find out whether there is any attack behavior that exploits the vulnerability in the traffic. When the system is upgraded to version V6.6.1.2 or above, the SSH brute force cracking function can be enabled to detect the attack behavior. The vulnerability rule base has been upgraded to version 2024070507 to detect this vulnerability.
Antiy Scalable Detection and Response Platform	Product function: Extended detection and response to the collected network and terminal log information. Attacks that exploit the vulnerability can be discovered. The vulnerability rule base has been upgraded to version 2024070401 to detect this vulnerability.
Antiy SCS（Security Code Scan）	Product function: Perform security checks on software source code to find out whether the vulnerability exists in the software. The vulnerability rule base has been upgraded to version 2.4.20240704.1 to detect this vulnerability.
Antiy Video System Security Comprehensive Assessment Equipment	Product function: Perform security checks on business applications to find out whether the vulnerability exists in the business applications. The vulnerability rule base has been upgraded to version 20240702114313 to detect this vulnerability.

If you need to obtain a product upgrade package, please call Antiy's technical support hotline: 400-840-9234.

Appendix: 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.