SECURITY ADVISORY

CYBER STASH

July, 2024

CVE-2024-6387

Exploiting the regreSSHion Vulnerability

Context

The identified vulnerability, known as "regreSSHion," impacts OpenSSH, a widely-deployed implementation of the Secure Shell (SSH) protocol pivotal for secure remote administration and file transfers within enterprises. This flaw permits remote, unauthenticated adversaries to execute arbitrary code on affected systems, thereby potentially compromising the confidentiality, integrity, and availability of the targeted infrastructure.

Designated as CVE-2024-6387, this vulnerability manifests as a race condition in the signal handler of OpenSSH, facilitating unauthenticated remote code execution with root privileges. Notably, this issue pertains specifically to the default configuration of sshd, thus posing a critical security threat necessitating immediate attention and remediation by organizations reliant on OpenSSH for secure communications.

Addressing this vulnerability can be effectively managed through proactive measures such as applying patches promptly or implementing network configurations that restrict direct internet access. If these controls are not feasible right away, you can reduce the risk by configuring the OpenSSH server to set the LoginGraceTime parameter to 0. This prevents unauthenticated sessions from staying open and being vulnerable to exploitation. Yet, this adjustment could potentially lead to a denial of service if all connection slots are filled.

Mitigation

Addressing the regreSSHion vulnerability requires immediate and proactive measures:

Patch Management: Apply the security patches released by OpenSSH maintainers immediately. Ensure that all systems are kept up-to-date to prevent exploitation.

Enhanced Access Control: Implement strict network-based controls to limit SSH access. Restrict SSH connections to trusted IP addresses using firewalls and security groups.

Blocking Network Traffic: Implement proactive network traffic blocking measures, including the restriction of suspicious IPs, domains, and connections from high-risk Autonomous System Numbers, Top-Level Domains, and countries.

Technical Details

Vulnerability

The newly discovered vulnerability in OpenSSH's server (sshd) arises from a signal handler race condition triggered when a client fails to authenticate within the designated LoginGraceTime period. Specifically, if this timeout threshold is surpassed, sshd's SIGALRM handler activates, invoking unsafe functions such as syslog() within a signal context, thereby posing a substantial security risk.

This flaw represents a regression of CVE-2006-5051, which was initially identified in 2006. The issue resurfaced in October 2020 with the release of OpenSSH 8.5p1, following the removal of a critical directive during an update to the logging infrastructure. This removal rendered sigdie() unsafe once more, leading to the current vulnerability.

Versions of OpenSSH exhibit varying degrees of vulnerability:

- OpenSSH versions prior to 4.4p1 are susceptible unless patched for CVE-2006-5051 or CVE-2008-4109.
- Versions from 4.4p1 to less than 8.5p1 are generally considered safe due to a safeguarding directive.
- However, versions from 8.5p1 to less than 9.8p1 are vulnerable again due to the removal of the directive.

This vulnerability poses heightened risks on glibc-based Linux systems, where exploitation could potentially result in arbitrary code execution as root without requiring authentication. This severity stems from sshd's privileged execution context, which operates with unrestricted system privileges and lacks sandboxing measures.

Exploitation

Exploiting the signal handler race condition in OpenSSH demands expertise in timing attacks and memory manipulation. The attacker initiates multiple connections, allowing the LoginGraceTime limit to trigger the SIGALRM signal in sshd deliberately. They meticulously disrupt timing during non-async-signal-safe operations like syslog() within the signal handler, aiming to manipulate heap memory. This involves executing around 10,000 connection attempts, strategically altering memory states during critical allocation or deallocation functions within sshd. Adjustments based on timing feedback refine the attack, overcoming defenses such as ASLR and NX protections. Successful exploitation grants remote root access by enabling arbitrary code execution on the server.

Tactics, Techniques and Procedures

The notable TTPs related to the DISGOMOJI are:

T1190 - Exploit Public-Facing Application

Attackers exploit the vulnerability in the public-facing SSH service.

T1059 - Command and Scripting Interpreter

After exploitation, attackers may use scripting interpreters like Bash or Python to execute further commands.

Furthermore, this vulnerability has the potential to facilitate network propagation, enabling attackers to leverage a compromised system as a stepping stone to traverse and exploit other vulnerable systems within the organization.

Cyber Threat Intelligence

Threat Actors

A range of threat actors, from opportunistic cybercriminals to sophisticated state-sponsored groups, may exploit the regreSSHion vulnerability due to its critical impact on secure communications.

Exploitation in the Wild

Over 14 million potentially vulnerable OpenSSH server instances have been identified as exposed to the Internet. Approximately 700,000 external internet-facing instances are vulnerable, representing 31% of all internet-facing OpenSSH instances in Qualys's global customer base.

References

Related IOC's & Yara Rules:

Autonomous System Numbers

CyberStash has detected attacks targeting this vulnerability originating from the listed Autonomous Systems:

DigitalOcean	Hurricane Electric LLC
CHINANET-BACKBONE	Alibaba (US) Technology Co.
Chang Way Technologies Co. Limited	CHINA UNICOM China169 Backbone
Emanuel Hosting Ltd.	China Education and Research Network Center
Korea Telecom	Limenet
Amarutu Technology Ltd	Censys
Hangzhou Alibaba Advertising Co.	China Mobile Communications Group Co.
Simple Carrier LLC	SCALEWAY S.A.S.
UAB Host Baltic	Shenzhen Tencent Computer Systems Company Limited

Public Intelligence:

- https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server
- https://www.darkreading.com/cloud-security/regresshion-bug-threatens-takeover-of-millions-of-linux-systems
- https://www.cyberdaily.au/security/10773-over-14-million-servers-could-be-vulnerable-to-newly-re-discovered-regresshion-flaw