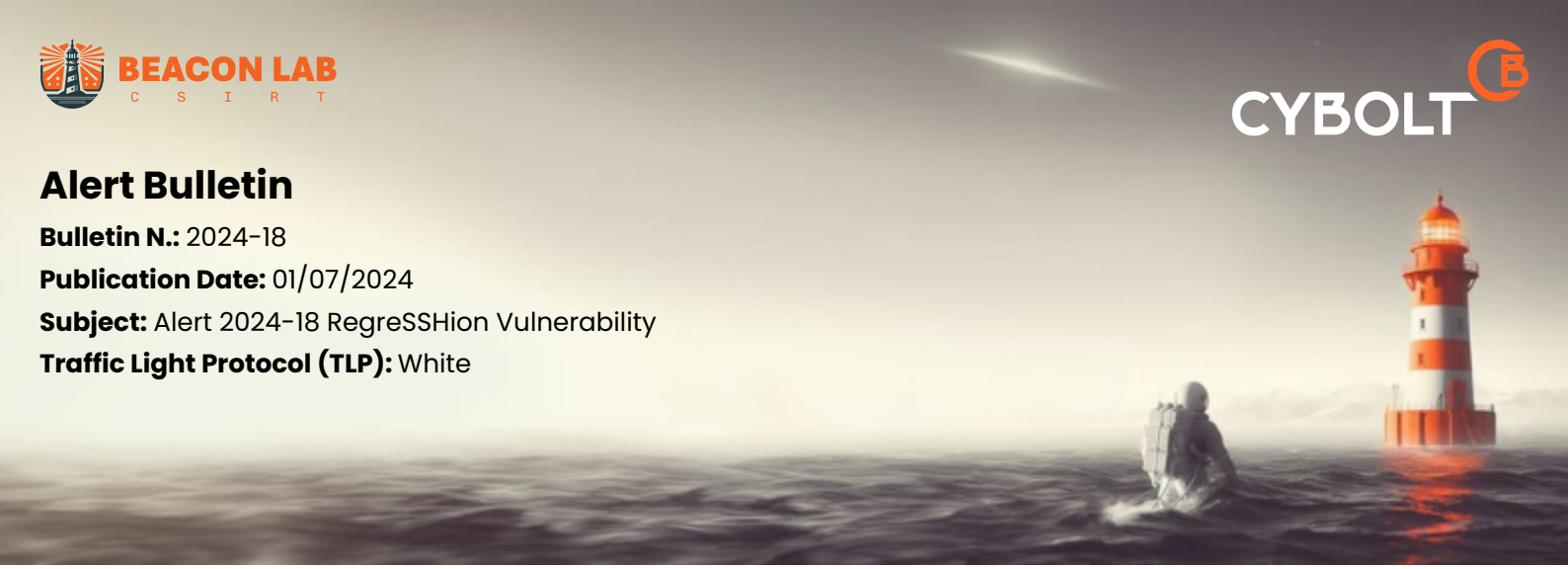

Alert Bulletin

Bulletin N.: 2024-18
Publication Date: 01/07/2024
Subject: Alert 2024-18 RegreSSHion Vulnerability
Traffic Light Protocol (TLP): White

Affected Product(s):

- Versions prior to **4.4p1**: Vulnerable if they do not have patches for **CVE-2006-5051** and **CVE-2008-4109**.
- Versions from **8.5p1** to **9.8p1**, not including 9.8p1: The vulnerability resurfaces due to the accidental removal of a critical component in a function.

Description:

The **Qualys Threat Research Unit (TRU)** has discovered a severe vulnerability named **"regreSSHion"** (CVE-2024-6387) affecting the **OpenSSH server (sshd)** on **glibc-based Linux systems**. This flaw, a race condition in the signal handler, allows unauthenticated attackers to gain root access and take full control of vulnerable machines. The vulnerability is a regression of **CVE-2006-5051**, a previously fixed issue that has resurfaced in later versions.

Researchers who developed an exploit for **AMD64** note that successful exploitation requires multiple attempts to win the race condition and that due to normal **ASLR** protections, successful exploitation is complex and slow. In their tests, it took them a week to obtain a root shell on the **x86 (32-bit)** version, and it has not been tested on **x64 (64-bit)**.

Prevention:

Successful exploitation of the "regreSSHion" vulnerability could have devastating consequences:

- **Complete System Compromise**: Attackers can install malware, manipulate data, and establish backdoors for persistent access.
- **Network Propagation**: The vulnerability allows attackers to bypass security mechanisms and spread throughout the network, putting both businesses and individuals at risk.

Mitigation:

- **Update OpenSSH** to version **9.8p1**, which fixes the vulnerability.

Compensatory Controls:

- **Modify sshd Configuration**: If updating or recompiling sshd is not possible, set **LoginGraceTime** to **0** in the sshd configuration file. This will make sshd vulnerable to denial of service but will mitigate the possibility of remote code execution.
- **Restrict SSH Access**:
- Configure firewalls to limit SSH access only to authorized IP addresses.
- Block SSH access from insecure or unnecessary locations.
- Limit SSH access to specific servers within those segments.
- Allow SSH access only from a predefined list of trusted IP addresses.