Security Advisory
"regreSSHion" OpenSSH vulnerability in PRC7000

1 Advisory Information

Advisory ID: BOSCH-SA-258444
CVE Numbers and CVSS v3.1 Scores:

- CVE-2024-6387
  - Base Score: 8.1 (High)

Published: 19 Jul 2024
Last Updated: 19 Jul 2024

2 Summary

The Qualys Threat Research Unit (TRU) [1] has discovered a Remote Unauthenticated Code Execution (RCE) vulnerability in OpenSSH's server (sshd) in glibc-based Linux systems. The vulnerability, which is a signal handler race condition in OpenSSH's server (sshd), allows unauthenticated remote code execution (RCE) as root on glibc-based Linux systems; that presents a significant security risk. This race condition affects sshd in its default configuration. (Excerpt from Qualys Community [2])

3 Affected Products

- PRC7000
  - CVE-2024-6387
    - Version(s): 1.11.12.0 <= 1.11.12.4
    - Version(s): 1.11.13.0 <= 1.11.13.1

4 Solution

Update the PRC7000 firmware to version 1.11.12.5 (or newer) or 1.11.13.2 (or newer). Please contact your key account manager for the availability of your firmware variant.

5 Mitigation

The issue can be mitigated via strict firewall rules to prevent arbitrary third parties from connecting to the PRC7000 SSH/SFTP port 22. Please note that the SFTP connection is mandatory for the PRI7000 software to be able to work with the PRC7000 control.

6 Vulnerability Details

6.1 CVE-2024-6387

CVE description: A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

- Problem Type:
  - CWE-364: Signal Handler Race Condition
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.1 (High)

7 Remarks

7.1 Security Update Information

With respect to Directive (EU) 2019/770 and Directive (EU) 2019/771 and their national transposition laws, please note:

It is your responsibility to download and/or install any security updates provided by us, for example to maintain product or data security. If you fail to install a security update provided to you within a reasonable period of time, we will not be liable for any product defect solely due to the absence of such security update.

Alternatively, we are entitled to directly download and/or install security updates regardless of your settings. In these cases, we will provide you with the relevant information, e.g., in this security advisory.

7.2 CVSS Scoring

Vulnerability classification has been performed using the CVSS v3.1 scoring system. The CVSS environmental score is specific to each customer's environment and should be defined by the customer to attain a final scoring.

8 Additional Resources

[1] Qualys Threat Research Unit (TRU)
https://www.qualys.com/tru/

[2] regreSSHion: Remote Unauthenticated Code Execution Vulnerability in Open SSH server
https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server

9 Revision History

19 Jul 2024: Initial Publication