Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 292 **19-07-2024**

Name: New OpenSSH Vulnerability Causes Remote Code Execution as Root on Linux Systems

Threat Classification: Vulnerability

Affected Software / Services:

- OpenSSH 8.5p1
- OpenSSH 9.7p1

Summary:

A vulnerability, identified as CVE-2024-6387, also known as regreSSHion, identifies a critical vulnerability in OpenSSH's sshd server component on Linux systems with glibc. This flaw could allow unauthenticated remote code execution (RCE) as root, potentially leading to full system compromise. OpenSSH maintainers have released security patches addressing this issue. Despite fixes, such vulnerabilities may reappear in subsequent releases due to inadvertent updates. It underscores the importance of rigorous regression testing to prevent reintroduction of known vulnerabilities.

Severity	**High**
Attack Vector	**Remote Code Execution**

Recommendations:

- It is highly advised to Upgrade to the latest version of OpenSSH, available from the OpenSSH Website.

https://www.openssh.com/releasenotes.html#9.8p1

- Users are strongly advised to apply updates promptly, implement network segmentation, and restrict SSH access to mitigate risks.
- Keep all the systems and software's up to date with the latest security patches to prevent attackers from exploiting known vulnerabilities.
- In case of any incident, please report to this office, through PTA CERT Portal and email.