UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0275

OPENSSH RELEASES SECURITY PATCH

DATE ISSUED: 7th February 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

OpenSSH released a security patch to address number of security bugs. OpenSSH supports open-source implementation of the Secure Shell (SSH) protocol that facilitate services for encrypted communications over an unsecured network in a client-server architecture.

BREAKDOWN

The security patch OpenSSH 9.2 contains fixes for two security problems and a memory safety problem. The vulnerability is tracked as CVE-2023-25136 and relates to a pre-authentication double-free memory fault introduced in OpenSSH 9.1. A double free memory flaw arises when a vulnerable piece of code calls the free() function which is used to deallocate memory function blocks - twice, leading to memory corruption. According to MITRE, double-freeing memory may result in write-what-where conditions, allowing an attacker to execute malicious code. However, the exploitation of this vulnerability is a difficult task due to protective measures placed by modern memory allocators.

REMEDIATION STEPS

- Update OpenSSH to the latest security patch.
- Monitor network activity for any suspicious or anomalous behaviour.

REFERENCES & RESOURCES

The Hacker News	https://thehackernews.com/2023/02/openssh-releases-patch-for-new-pre-auth.html?_m=3n%2e009a%2e2959%2eyv0ao44qnr%2e1xkm
OpenSSH Release Notes	https://www.openssh.com/releasenotes.html