National Cyber Security Centre

2407010161-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Remote Unauthenticated Code Execution Vulnerability in OpenSSH

Monday 1st July, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

The Qualys Threat Research Unit (TRU)[1] have discovered a Remote Unauthenticated Code Execution (RCE) vulnerability in OpenSSH's server (sshd) in glibc-based Linux systems. The CVE assigned to this vulnerability is CVE-2024-6387.

The vulnerability is known as regreSSHion and if it is successfully exploited, the attacker can obtain unlimited root-level access to vulnerable systems.

More information from TRU can be found here: https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server.

Products Affected

On Linux systems:

- Versions of OpenSSH starting from 8.5p1 and prior to version 9.8p1.
- Versions of OpenSSH prior to 4.4p1.

OpenBSD-based systems are not vulnerable.

Impact

Exploitation of CVE-2024-6387 could allow full system compromise where an attacker can execute arbitrary code with root level access which can lead to complete system takeover, installation of malware, data manipulation, and the creation of backdoors for persistent access. It could also facilitate network propagation, allowing attackers to use a compromised system as a foothold to traverse and exploit other vulnerable systems within the organisation.

Recommendations

The NCSC strongly advises affected organisations to identify any assets that are running OpenSSH and identify vulnerable versions. The software supplier has released a corrective update, which should be installed as soon as possible.

Further information and some steps that organisations can take can be found here:

- https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server
- https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt
- https://www.openssh.com/txt/release-9.8

[1] https://www.qualys.com/tru/

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre