Network Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

See what the DEEP scanner can do

Perform in-depth scanning and detect a wider range of vulnerabilities.

Scanner capabilities	Light scan	Deep scan
Open ports detection	✓	✓
Version based vulnerability detection	✓	✓
Active vulnerability detection (57000+ plugins)	✗	✓
Find service misconfigurations	✗	✓
Detect missing security patches	✗	✓

✓ **openssh.pentest-ground.com**

The Light Network Scanner only ran limited, version-based detection. Upgrade to run Deep scans that check for 20,000+ additional vulnerabilities - with fewer False Positives

Summary

Overall risk level:

High

Risk ratings:

High:	1
Medium:	0
Low:	0
Info:	3

Scan information:

Start time:	Jul 03, 2024 / 16:40:15
Finish time:	Jul 03, 2024 / 16:41:04
Scan duration:	49 sec
Tests performed:	4/4
Scan status:	Finished

Findings

OpenSSH - Remote Code Execution (CVE-2024-6387)

port 22/tcp

CONFIRMED

We extracted the following information from the target: **8.9p1**
Endpoint: **openssh.pentest-ground.com:22**

Details

Vulnerability description:

An incorect management of a signal handler race condition was found in OpenSSH's server. A remote attacker could use this issue to bypass authentication using sshd's SIGALRM handler. However, this signal handler calls various functions that are not async-signal-safe, which could lead to undeterministic behavior.This vulnerability can be remotely exploited on glibc-based Linux systems where syslog() invokes async-signal-unsafe functions like malloc() and free(). It allows for unauthenticated remote code execution as root because it impacts the privileged code of sshd, which runs with full privileges and is not sandboxed.

Risk description:

The risk exists that a remote unauthenticated attacker can fully compromise the server to steal confidential information, install

ransomware, or pivot to the internal network.

Recommendation:
We recommend upgrading the affected software to the 9.8p1 version or higher which mitigates this vulnerability.

References:
https://pentest-tools.com/network-vulnerability-scanning/cve-2024-6387-scanner-regresshion-vulnerability
https://pentest-tools.com/blog/regresshion-cve-2024-6387
https://stackdiary.com/openssh-race-condition-in-sshd-allows-remote-code-execution/
https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt
https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2024-6387
https://ubuntu.com/security/cve-2024-6387
https://access.redhat.com/security/cve/cve-2024-6387

IP Information

CONFIRMED

IP Address	Hostname	Location	Autonomous system (AS) Information	Organization (Name & Type)
70.34.243.198	openssh.pentest-ground.com	Warsaw, Mazowieckie, Poland	The Constant Company LLC (AS20473)	The Constant Company LLC (hosting)

Details

Risk description:
If an attacker knows the physical location of an organization's IP address and its Autonomous System (AS) number, they could launch targeted physical or cyber attacks, exploiting regional vulnerabilities or disrupting critical infrastructure.

Recommendation:
We recommend reviewing physical security measures and monitoring network traffic for unusual activity, indicating potential cyber threats. Additionally, implementing robust network segmentation and adopting encryption protocols for data in transit can help protect sensitive information, even if attackers are aware of the IP addresses and the Autonomous System (AS) number.

DNS Records

CONFIRMED

DNS Record Type	Description	Value
A	IPv4 address	70.34.243.198

Details

Risk description:
An initial step for an attacker aiming to learn about an organization involves conducting searches on its domain names to uncover DNS records associated with the organization. This strategy aims to amass comprehensive insights into the target domain, enabling the attacker to outline the organization's external digital landscape. This gathered intelligence may subsequently serve as a foundation for launching attacks, including those based on social engineering techniques. DNS records pointing to services or servers that are no longer in use can provide an attacker with an easy entry point into the network.

Recommendation:
We recommend reviewing all DNS records associated with the domain and identifying and removing unused or obsolete records.

Open ports discovery

CONFIRMED

Port	State	Service	Product	Product Version
22	open	ssh	OpenSSH	8.9p1 Ubuntu 3ubuntu0.10

Details

Risk description:
This is the list of ports that have been found on the target host. Having unnecessary open ports may expose the target to more risks because those network services and applications may contain vulnerabilities.

Recommendation:
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

Scan coverage information

List of tests performed (4/4)

- ✔ Running IP information lookup phase...
- ✔ DNS enumeration
- ✔ Port discovery
- ✔ Checking for OpenSSH - Remote Code Execution (CVE-2024-6387) (Nuclei Template) on port 22

Scan parameters

Target:	openssh.pentest-ground.com
Preset:	Custom
Scanning engines:	Nuclei
Check alive:	False
Extensive modules:	-
Protocol type:	TCP
Ports to scan:	22