Check Point Remote Access VPN vulnerability

May 2024

SOC Informative Report

Document details

Title of the activity
Check Point Remote Access VPN vulnerability

Summary
Report containing information about a critical vulnerability discovered in Check Point Security Gateways

Target audience

SOC and SOC AdS representatives

Confidentiality level (Clear/Green/Amber/Amber+Strict/Red)
CLEAR

Publication date
30/05/2024

Written by
Mirko Ioris, Luca Zeni

Reviewed by
Massimo Giaimo

Confidentiality level

A level of confidentiality is applied to the document, marked by the "Confidentiality Level" item on the front page. The values that can be used (RED / AMBER / AMBER+STRICT / GREEN / CLEAR) have the following meanings:

TLP:RED = Reserved for participants only.

> Sources may use TLP:RED when the information cannot be effectively used by other parties and could impact a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with parties outside the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most cases, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

TLP:AMBER+STRICT limits sharing to the *organization* only.

> Sources may use TLP:AMBER when the information requires support to act effectively but poses risks to privacy, reputation, or operations if shared outside the organizations involved. Recipients may share TLP:AMBER information only with members of their own organization and with clients or customers who need to know the information to protect themselves or prevent further harm.
>
> Note: If the source wishes to limit sharing **only** to the organization, it must specify TLP:AMBER+STRICT.

TLP:GREEN =Limited disclosure, restricted to the community.

> Sources may use TLP:GREEN when the information is useful for the awareness of all participating organizations, as well as with colleagues within the community or broader sector. Recipients may share TLP:GREEN information with colleagues and partner organizations within their sector or community, but not through publicly accessible channels. Information in this category may be widely disseminated within a particular community. TLP:GREEN information may not be released outside the community.

TLP:CLEAR = Disclosure is not limited.

Sources may use TLP:CLEAR when the information poses little or foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.

Table of contents

Check Point Remote Access VPN vulnerability 0
Document details 1
Confidentiality level 2
Table of contents 4
Introduction 5
Attack surface 6
IOC 7
Affected products 8
Remediation 9
Bibliography 10

Introduction

The **Check Point Research Division** discovered a security vulnerability in Security Gateways with IPsec VPN, Remote Access VPN or the Mobile Access blade enabled. A hotfix was released on May 28 to fix the vulnerability [1].

Check Point classified the vulnerability as **Information Disclosure** and assigned it the CVE number **CVE-2024-24919** [2]. It was initially published with a CVSS score of 7.5, later increased to 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).

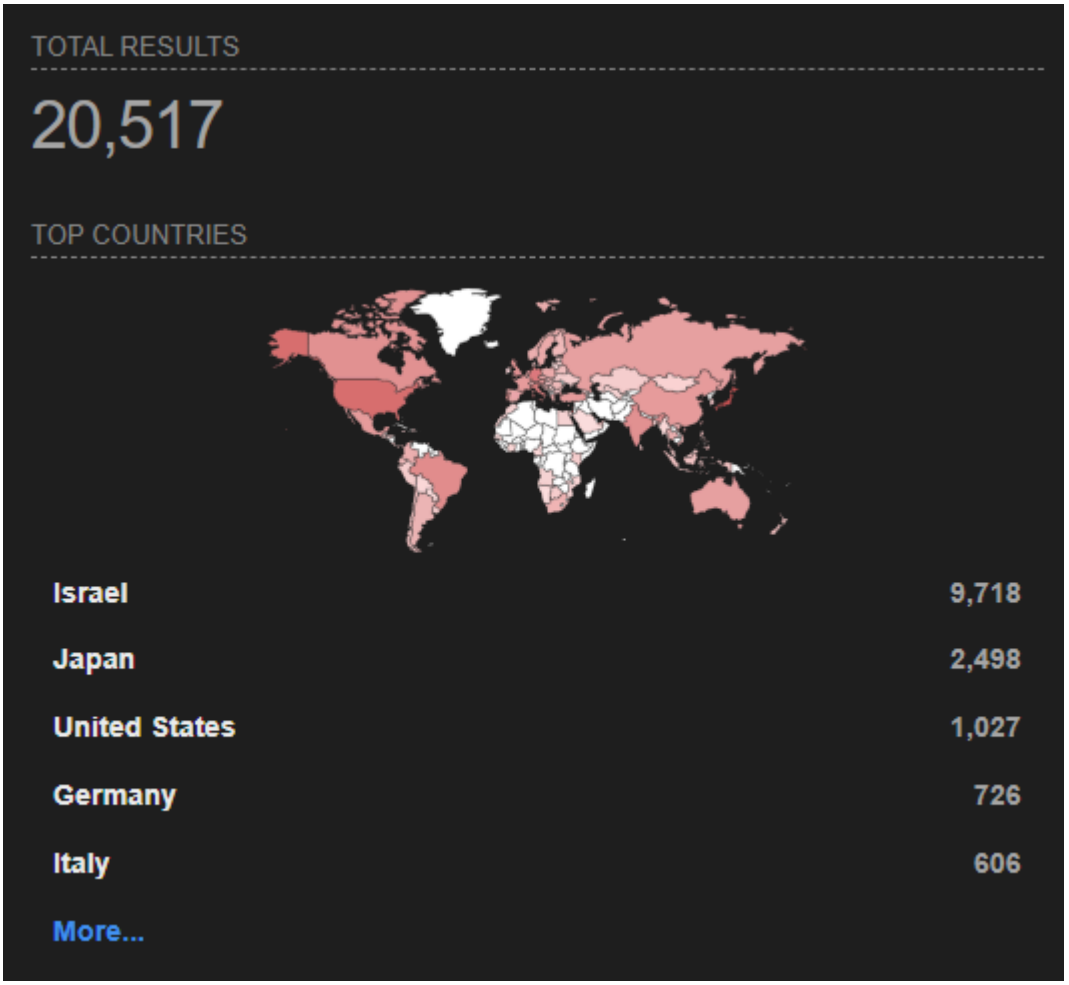
CVE Number	CVSS Score	EPSS Score
CVE-2024-24919	8.6 (High)	0.04% (Low)

The vulnerability has a HIGH severity, but what it allows an attacker to do is very critical. Security experts at **watchTowr** [3] reverse engineered the CVE, discovering that it's in truth a path traversal leading to an arbitrary file reading with superuser rights. This potentially allows a remote attacker to read anything on the filesystem they target.

Attack surface

The following are Check Point Internet-exposed devices found with **Shodan** that are vulnerable if not updated (search date 30/05/2024):

Shodan Query
http.title:"Check Point SSL Network Extender"



IOC

Check Point [4] and **mnemonic** [5] observed multiple usage of the exploit being used in the wild. A list of IOC is here reported (last update 30 May):

23.227.196.88	158.62.16.45	82.180.133.120
23.227.203.36	167.61.244.201	146.185.207.0/24
37.19.205.180	178.236.234.123	193.233.128.0/22
38.180.54.104	185.213.20.20	193.233.216.0/21
38.180.54.168	185.217.0.242	217.145.225.0/24
46.59.10.72	192.71.26.106	31.134.0.0/20
46.183.221.194	195.14.123.132	37.9.40.0/21
46.183.221.197	203.160.68.12	45.135.1.0/24
64.176.196.84	68.183.56.130	45.135.2.0/23
87.206.110.89	167.99.112.236	45.155.166.0/23
104.207.149.95	132.147.86.201	5.188.218.0/23
109.134.69.241	162.158.162.254	85.239.42.0/23
146.70.205.62	61.92.2.219	88.218.44.0/24
146.70.205.188	183.96.10.14	91.132.198.0/24
149.88.22.67	198.44.211.76	91.218.122.0/23
154.47.23.111	221.154.174.74	91.245.236.0/24
156.146.56.136	112.163.100.151	
87.120.8.173	103.61.139.226	

Affected products

The affected products and its versions are shown below:

- **Security Gateway** and **CloudGuard Network Security**
  - R81.20
  - R81.10
  - R81
  - R80.40
- **Quantum Maestro** and **Quantum Scalable Chassis**
  - R81.20
  - R81.10
  - R80.40
  - R80.30SP
  - R80.20SP
- **Quantum Spark Gateways**
  - R81.10.x
  - R80.20.x
  - R77.20.x

Remediation

The **Check Point Research Division** has already published a hotfix to prevent exploits of CVE-2024-24919, available for all the compromised product and version.

Step by step guide https://support.checkpoint.com/results/sk/sk182336

It' also recommended to perform the following actions:

- Change the password of the LDAP Account Unit
- Reset password of local accounts connecting to VPN with password authentication
- Prevent Local Accounts from connecting to VPN with Password Authentication
- Renew Security Gateway's Outbound SSL Inspection CA certificate
- Renew Security Gateway's Inbound SSL Inspection server certificates
- Reset all Gaia OS admin, local users and Expert mode passwords

Bibliography

[1]https://support.checkpoint.com/results/sk/sk182336

[2]https://nvd.nist.gov/vuln/detail/CVE-2024-24919

[3]https://labs.watchtowr.com/check-point-wrong-check-point-cve-2024-24919/#/

[4]https://support.checkpoint.com/results/sk/sk182337

[5]https://www.mnemonic.io/resources/blog/advisory-check-point-remote-access-vpn-vulnerability-cve-2024-24919/