BEACON LAB
CSIRT

CYBOLT

Alert Bulletin

Bulletin N.: 2024-13
Publication Date: 31/05/2024
Subject: Alert 2024-13 Critical Vulnerability in Check Point VPN
Traffic Light Protocol (TLP): White

Affected Product(s):

- Check Point Security Gateways with remote access VPN or Mobile Access Software Blades enabled.

Description:

Check Point has recently released a security patch for a zero-day vulnerability in the VPN module that has been exploited by attackers to gain remote access to firewalls and attempt to compromise internal networks.

This vulnerability, identified as **CVE-2024-24919**, has a severity score of **8.6**, as it allows attackers to exploit this vulnerability remotely.

It is important to note that a patch is already available that fully addresses this issue on the device; therefore, it is highly recommended that all users apply the patch as soon as possible.

Additionally, the manufacturer has reported a significant increase in attacks on their products since **Monday, May 27**, shortly after discovering that these attacks were linked to the aforementioned vulnerability.

Impact:

A malicious actor who can remotely access the aforementioned applications could exploit this flaw, gaining access to the device, which they could then use to extend their attack throughout the corporate network.

Solution:

Apply the official patch published by Check Point.

Additional Information:

- Bleeping Computer Article
- NVD CVE-2024-24919

- **The Hacker News Article**