THREAT REPORT: Check Point Network Gateway Vulnerability

June 5, 2024

TLP: WHITE

Source: Important Security Update – Stay Protected Against VPN Information Disclosure (CVE-2024-24919) | Check Point Blog

Overview:

On 27th May 2024, Check Point disclosed a zero-day arbitrary file read vulnerability tracked as CVE-2024-24919 which affects multiple Check Point network gateway devices. Security patches were also released at the same time to remediate the flaw which, according to Check Point, only affected devices that have remote access virtual private network (VPN), or mobile access enabled.

The vulnerability was originally discovered because of an investigation by defenders at Check Point looking into suspicious login activity. Check Point observed multiple login attempts to VPN devices using local accounts that rely on single factor authentication.

The threat actors responsible were able to authenticate by leveraging the vulnerability to perform a path traversal into the filesystem containing the shadow password file. This enables the threat actors to extract any passwords available on compromised devices which can be used to gain access to systems that are configured with single factor authentication.

Researchers at watchTowr Labs recreated a working exploit that led to accessing the filesystem containing the shadow password file. Their technical analysis also demonstrated that doing so would grant them superuser privileges. This meant the vulnerability could also provide a means for privilege escalation, increasing the severity of the vulnerability in many systems.

Immediately following the announcement by Check Point, GoA CTI analysts discovered a high number of systems running some version of Check Point network gateway products. Some were found within the GoA's infrastructure, and many more internet facing gateways were found across the province by using web crawler platforms.

As the vulnerability was a zero-day, it was assessed that all discovered systems were almost certain to be unpatched. The threat was then increased with the subsequent release of the proof-of-concept by watchTowr Labs, demonstrating to any would-be threat actors how they could successfully exploit the vulnerability.

What to Communicate to Executives:

- **Investigate Potential Exposure:** GoA CTI recommends that all owners of a Check Point network gateway product review the security update provided by Check Point and determine if their version is affected or not.
- **Updating:** Installing the appropriate security update for any affected versions should immediately take place. Failing to do so will leave valuable password files, and potentially privileged access footholds available to threat actors.

Further Reading:

- Important Security Update – Stay Protected Against VPN Information Disclosure (CVE-2024-24919) | Check Point Blog
- Preventative Hotfix for CVE-2024-24919 - Quantum Gateway Information Disclosure | Check Point
- Check Point - Wrong Check Point (CVE-2024-24919) | watchTowr Labs
- Check Point Warns of Zero-Day Attacks on its VPN Gateway Products | The Hacker News

CYBER ALBERTA