f

(/Application/Dashboard/Dashboard)

Welcome Mayya Jabbour-Saab Logout (/Application/Account/Logoff)

——All

A VULNERABILITY IN CHECK POINT SECURITY GATEWAYS COULD ALLOW FOR CREDENTIAL ACCESS

Posted Date: 06/03/2024
Published Date: 05/31/2024
Source: MS-ISAC
Number Of Views: 17.
Average Rating: .
0 members have rated this article.
Rate the article : ★★★★★

TLP:CLEAR
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2024-065

DATE(S) ISSUED: 05/31/2024

SUBJECT: A Vulnerability in Check Point Security Gateways Could Allow for Credential Access

OVERVIEW:

A vulnerability has been discovered in Check Point Security Gateway Products that could allow for credential access. A Check Point Security Gateway sits between an organization’s environment and the Internet to enforce policy and block threats and malware. Successful exploitation of this vulnerability could allow for credential access to local accounts due to an arbitrary file read vulnerability. Other sensitive files such as SSH keys and certificates may also be read. Depending on the privileges associated with the accounts, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Local accounts that are configured to have fewer rights on the system could be less impacted than those that operate with administrative rights.

THREAT INTELLIGENCE: Check Point is aware that an exploit for CVE-2024-24919 exists in the wild and is being actively exploited. Additionally, the cybersecurity organization mnemonic has reported observing threat actors extracting ntds.dit, a store of Active Directory hashes on a Domain Controller, from compromised customers within 2-3 hours after logging in with a local user.

SYSTEMS AFFECTED:

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

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Check Point Security Gateway Products that could allow for credential access. The vulnerability affects Security Gateway products making use of the IPsec VPN or Mobile Access. Exploiting this vulnerability can result in accessing arbitrary files on the system including /etc/shadow which contains password hashes for local accounts on the Security Gateway. The hashes can be cracked and allow for the attacker to authenticate as those users, allowing for lateral movement and the potential to gain domain admin privileges. Details of the vulnerability are as follows:

Tactic: *Credential Access* **(**TA0006 (https://learn.cisecurity.org/e/799323/tactics-TA0006-/4tpcrb/2160524316/h/YbivXxE31sk8iU1a6DFe6HZdTyIROvT1RIiCPNz5fp8)**):**
Technique: *Exploitation for Credential Access* **(**T1212 (https://learn.cisecurity.org/e/799323/techniques-T1212-/4tpcrf/2160524316/h/YbivXxE31sk8iU1a6DFe6HZdTyIROvT1RIiCPNz5fp8)**):**

- Arbitrary file read vulnerability (CVE-2024-24919)

Successful exploitation of this vulnerability could allow for credential access to local accounts due to an arbitrary file read vulnerability. Other sensitive files such as SSH keys and certificates may also be read. Depending on the privileges associated with the accounts, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Local accounts that are configured to have fewer rights on the system could be less impacted than those that operate with administrative rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply the updates provided by Check Point to vulnerable systems immediately after appropriate testing. (**M1051 (https://learn.cisecurity.org/e/799323/mitigations-M1051/4tpcrj/2160524316/h/YbivXxE31sk8iU1a6DFe6HZdTylROvT1RliCPNz5fp8): Update Software**)
    - **Safeguard 7.1 : Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.2 : Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **Safeguard 7.6 : Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets:** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
    - **Safeguard 7.7 : Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - **Safeguard 16.13 Conduct Application Penetration Testing:** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.
    - **Safeguard 18.1 : Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
    - **Safeguard 18.2 : Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and

    experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
    - **Safeguard 18.3 : Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise’s policy for remediation scope and prioritization.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026** (https://learn.cisecurity.org/e/799323/mitigations-M1026/4tpcrm/2160524316/h/YbivXxE31sk8iU1a6DFe6HZdTyIROvT1RIiCPNz5fp8)**: Privileged Account Management**)
-
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user’s primary, non-privileged account.

REFERENCES:

Check Point:
https://support.checkpoint.com/results/sk/sk182336
(https://support.checkpoint.com/results/sk/sk182336)
https://blog.checkpoint.com/security/enhance-your-vpn-security-posture/
(https://blog.checkpoint.com/security/enhance-your-vpn-security-posture/)

Rapid7:
https://www.rapid7.com/blog/post/2024/05/30/etr-cve-2024-24919-check-point-security-gateway-information-disclosure (https://www.rapid7.com/blog/post/2024/05/30/etr-cve-2024-24919-check-point-security-gateway-information-disclosure)

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

Bleeping Computer:
https://www.bleepingcomputer.com/news/security/check-point-releases-emergency-fix-for-vpn-zero-day-exploited-in-attacks/ (https://www.bleepingcomputer.com/news/security/check-point-releases-emergency-fix-for-vpn-zero-day-exploited-in-attacks/)

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24919 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24919)

Back

QUICK LINKS

DASHBOARD (/APPLICATION/DASHBOARD/DASHBOARD)
INBOX (/APPLICATION/MEMBER/VIEWMESSAGES)
MY PROFILE
CHANGE PASSWORD (/APPLICATION/MEMBER/CHANGEPASSWORD)
MY LOCATION (/APPLICATION/MEMBER/BRANCH/115)
FAQ (/CONTENT/FAQ.DOCX)
(/)
TERMINATE MEMBERSHIP (/APPLICATION/USERPROFILE/TERMINATEMEMBERSHIP)
DOWNLOAD MEMBERSHIP CARD (/APPLICATION/DASHBOARD/MEMBERSHIPCARD)
CONTACT US (/APPLICATION/MEMBER/CONTACTUS)

ALERTS (/APPLICATION/MEMBER/ALERTS)
ALL PUBLICATIONS (/APPLICATION/MEMBER/NEWSITEMS)
FBI REPORT (/APPLICATION/MEMBER/NEWSITEMS?C=1)
GENERAL INTEL REPORTS (/APPLICATION/MEMBER/NEWSITEMS?C=2)
FLASH & PINS (/APPLICATION/MEMBER/NEWSITEMS?C=1014)
NEWS (/APPLICATION/MEMBER/NEWSITEMS?C=1016)
USER POLICY GUIDELINES (/APPLICATION/MEMBER/USERPOLICY)
NON-DISCLOSURE AGREEMENT

SPEAKER BUREAU (/APPLICATION/USERPROFILE/USERLIST?SP=1)
LOCATIONS (/APPLICATION/BRANCH/CHAPTERLIST)
NATIONAL SECTOR SECURITY AND RESILIENCE PROGRAM (/APPLICATION/BRANCH/SECTORLIST)
CROSS-SECTOR COUNCILS (/APPLICATION/BRANCH/SIGLIST)
FORUMS (/APPLICATION/FORUM/FORUMS)
SUBMIT CYBER INCIDENT REPORT (/APPLICATION/MEMBER/GUARDIAN)
WEBINARS/VIDEOS (/APPLICATION/MEMBER/TRAINING)
INFRAGARD FACT SHEET (/CONTENT/INFRAGARDFACTSHEET_MARCH2024_ELECTRONICUSE.PDF)
BROCHURE (/CONTENT/INFRAGARD_BROCHURE_2024_UPDATE2.PDF)
LOGO GUIDELINES (/CONTENT/IGCONTENT/FBI_LOGO_GUIDELINES.PDF)
INFRAGARD NATIONAL MEMBERS ALLIANCE (HTTP://WWW.INFRAGARDMEMBERS.ORG)

CCIPS (HTTP://WWW.JUSTICE.GOV/CRIMINAL-CCIPS/CCIPS-DOCUMENTS-AND-REPORTS)

FTC SENTINEL (HTTPS://REGISTER.CONSUMERSENTINEL.GOV)

US SECRET SERVICE (HTTP://WWW.SECRETSERVICE.GOV)

NATIONAL COUNTER INTELLIGENCE AND SECURITY CENTER (HTTPS://WWW.NCSC.GOV/INDEX.HTML)

FBI.GOV (HTTPS://WWW.FBI.GOV/)

FTC.GOV (HTTPS://WWW.FTC.GOV/)

IC3.GOV (HTTPS://WWW.IC3.GOV/)

DHS (HTTPS://WWW.DHS.GOV/)

DSAC (HTTPS://WWW.DSAC.GOV/)

OSAC (HTTPS://WWW.OSAC.GOV/PAGES/HOME.ASPX)

US-CERT.ORG (HTTPS://WWW.US-CERT.GOV/)

NCFTA.ORG (HTTPS://WWW.NCFTA.NET/)

STAYSAFEONLINE.ORG (HTTPS://STAYSAFEONLINE.ORG/)

s1 124