29/05/2024
כ"א אייר תשפ"ד
[עדכון]
30/05/2024
כ"ב אייר תשפ"ד
סימוכין: 1743B

[עדכון] התרעה דחופה: פגיעות במוצרי צ'קפוינט עלולה לאפשר קריאת מידע רגיש ללא צורך בהזדהות

תקציר

1. צ'קפוינט פרסמה מידע לגבי פגיעות העלולה לאפשר לתוקף קריאת מידע רגיש ללא צורך בהזדהות.
2. הפגיעות מנוצלת בפועל בעולם על ידי תוקפים.
3. יש לבחון ולהתקין את הגרסאות העדכניות של המוצרים הפגיעים בהקדם האפשרי.

פרטים

1. הפגיעות מזוהה כ-CVE-2024-24919. ציון CVSS 8.6 (גבוה).
2. בקישור מס' 3 להלן מצוין כי קיימת אפשרות ש- **account data and hashes** could be potentially exfiltrated.
3. [עדכון] המוצרים הפגיעים הם:

1. ANY Security Gateway that has EITHER of the following setups:
    1. The IPsec VPN Blade is enabled, but ONLY when included in the Remote Access VPN community.
    2. The Mobile Access Software Blade is enabled.

דרכי התמודדות

1. יש לבחון ולהתקין בהקדם האפשרי את הגרסה העדכנית ביותר המתאימה למוצרים שברשותכם.
2. הגרסאות העדכניות הזמינות למשתמשים הן:

1. Quantum Security Gateway and CloudGuard Network Security Versions: R81.20, R81.10, R81, R80.40
2. Quantum Maestro and Quantum Scalable Chassis: R81.20, R81.10, R80.40, R80.30SP, R80.20SP
3. Quantum Spark Gateways Version: R81.10.x, R80.20.x, R77.20.x

3. [עדכון] מומלץ מאד לבחון ולבצע את הצעדים הבאים המומלצים על ידי החברה:

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

4. מומלץ מאד לבחון הלוגים לזיהוי תקיפות אפשריות כנגד הציוד.
5. [עדכון] פרטים כיצד לבצע את סעיפים 3 ו-4 לעיל, ניתן למצוא בקישורים מס' 2 ו-3 להלן.
6. [עדכון] בקישור מס' 3 להלן ציינה החברה רשימת כתובות וטווחי כתובות בפורמט CIDR, שהיו מעורבים בניצול הפגיעות. מומלץ לבחון האם לחסום או לנטר תעבורה מכתובות אלו. תשומת לב כי לפי מידע שבידי מערך הסייבר הלאומי, הכתובות הבאות מהרשימה הן של שירותי VPN או Proxy:

- 37.19.205.180 - Surfshark VPN
- 46.59.10.72 - Proxy
- 46.183.221.194 - Perfect Privacy VPN
- 46.183.221.197 - Perfect Privacy VPN
- 109.134.69.241 - Proxy
- 146.70.205.62 - Surfshark VPN
- 146.70.205.188 - Surfshark VPN
- 149.88.22.67 - Surfshark VPN
- 154.47.23.111 - Surfshark VPN

- 156.146.56.136 - Surfshark VPN
- 158.62.16.45 - Proxy
- 185.213.20.20 - Proxy
- 192.71.26.106 - Proxy?

7. מערך הסייבר הלאומי ממליץ כי כל גישה לציוד VPN הנגיש מרשת האינטרנט, תחייב הזדהות חזקה (2 Factor Authentication) עבור כלל משתמשי הציוד.

מקורות

1. https://blog.checkpoint.com/security/enhance-your-vpn-security-posture/
2. https://support.checkpoint.com/results/sk/sk182336
3. https://support.checkpoint.com/results/sk/sk182337
4. https://www.mnemonic.io/resources/blog/advisory-check-point-remote-access-vpn-vulnerability-cve-2024-24919/
5. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24919
6. https://nvd.nist.gov/vuln/detail/CVE-2024-24919
7. https://www.tenable.com/blog/cve-2024-24919-check-point-security-gateway-information-disclosure-zero-day-exploited-in-the

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו.
המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.