18 ספטמבר 2019
י"ח אלול תשע"ט
עדכון: 07 אוקטובר 2019
ח' תשרי תש"פ
סימוכין:ב-ס-995A

הרחבה בנושא הפגיעויות בציוד SSLVPN של חברת Pulse [עדכון]

תקציר

בהמשך להתרעת מערך הסייבר הלאומי בנושא פגיעויות במספר מוצרי SSLVPN, מסמך זה ירחיב המידע בנושא הסיכונים ודרכי ההתמודדות של משתמשי המוצר Pulse Connect Secure.

פרטים

1. לאחרונה פורסם כי ציוד SSLVPN של Pulse Secure חשוף לפגיעויות העלולות לאפשר לתוקף מרוחק ובלתי-מזוהה הרצת קוד על הציוד, או קריאה של קבצים מהציוד, כולל פרטי הזדהות של משתמשים (במקרים מסוימים אף פרטי המשתמש ב- Active Directory, אם הוגדרה הזדהות באמצעות פרטים אלו), או ביצוע פעולות בציוד בהרשאות Admin.
2. תוקף אף עלול להגדיר הרצת קוד על עמדות משתמש המתחברות לציוד ה- VPN, וכך להשיג אחיזה גם בהן.
3. לחלק מהפגיעויות קיים POC או מידע טכני נגיש ברשת, וחלקן ניתנות למימוש באמצעות גישה ל- URL מסוים על ציוד ה- VPN. [עדכון] ישנם ברשת Exploits לפגיעויות אלו.
4. מדובר באוסף של פגיעויות:

- **CVE-2019-11510 - Pre-auth Arbitrary File Reading**
- CVE-2019-11542 - Post-auth(admin) Stack Buffer Overflow
- **CVE-2019-11539 - Post-auth(admin) Command Injection**

- CVE-2019-11538 - Post-auth(user) Arbitrary File Reading via NFS
- CVE-2019-11508 - Post-auth(user) Arbitrary File Writing via NFS
- CVE-2019-11540 - Post-auth Cross-Site Script Inclusion
- CVE-2019-11507 - Post-auth Cross-Site Scripting

שילוב 2 הפגיעויות המודגשות (11510, 11539) הוא בעל פוטנציאל הנזק הגבוה ביותר.

5. המוצרים הפגיעים הם:

Pulse Connect Secure and Pulse Policy Secure

Pulse Connect Secure 9.0R1 - 9.0R3.3

Pulse Connect Secure 8.3R1 - 8.3R7

Pulse Connect Secure 8.2R1 - 8.2R12

Pulse Connect Secure 8.1R1 - 8.1R15

Pulse Policy Secure 9.0R1 - 9.0R3.3

Pulse Policy Secure 5.4R1 - 5.4R7

Pulse Policy Secure 5.3R1 - 5.3R12

Pulse Policy Secure 5.2R1 - 5.2R12

Pulse Policy Secure 5.1R1 - 5.1R15

דרכי התמודדות

שינויים בהגדרות ציוד מומלץ ליישם לאחר בחינה במערכות ניסוי.

1. **מומלץ לבחון ולהתקין את עדכוני האבטחה הרלוונטיים בהקדם האפשרי.**
2. להלן פרטי הגרסאות העדכניות:

Pulse Connect Secure and Pulse Policy Secure 9.1R1 and above

עבור גרסאות ישנות יותר ניתן לעדכן לפי הפירוט הבא:

גרסה מותקנת	ניתן לעדכן לגרסה זו או גבוהה ממנה
Pulse Connect Secure 9.0RX	Pulse Connect Secure 9.0R3.4 & 9.0R4

Pulse Connect Secure 8.3RX	Pulse Connect Secure 8.3R7.1
Pulse Connect Secure 8.2RX	Pulse Connect Secure 8.2R12.1
Pulse Connect Secure 8.1RX	Pulse Connect Secure 8.1R15.1
Pulse Policy Secure 9.0RX	Pulse Policy Secure 9.0R3.2 & 9.0R4
Pulse Policy Secure 5.4RX	Pulse Policy Secure 5.4R7.1
Pulse Policy Secure 5.3RX	Pulse Policy Secure 5.3R12.1
Pulse Policy Secure 5.2RX	Pulse Policy Secure 5.2R12.1
Pulse Policy Secure 5.1RX	Pulse Policy Secure 5.1R15.1

3. לאחר העדכון, **מומלץ מאד** לאתחל את סיסמאות הגישה לכלל המשתמשים בציוד ה- VPN.
4. לאחר העדכון, **מומלץ מאד** לחייב המשתמשים להזדהות מחדש.
5. מומלץ מאד לבחון שימוש בהזדהות דו-שלבית בגישה ל- VPN הארגוני.
6. **מומלץ מאד** להגדיר מחיקה של ה- Cache בעמדת הלקוח עם סיום ההתקשרות. הגדרה זו מופיעה תחת הכותרת Cache Cleaner (Authentication > Endpoint Security > Cache Cleaner).
7. **מומלץ מאד** להגדיר מחיקה של ה- Session Cookie בדפדפן של הלקוח באמצעות ההגדרה Users --> User Roles --> <role name> --> General --> Session Options: Remove Browser Session Cookie
8. מומלץ לאכוף שימוש בדיסק מוצפן בצד הלקוח. ניתן לבצע זאת באמצעות הגדרה של Predefined Hard Disk Encryption Rule.
9. **מומלץ מאד** לוודא כי רישום הלוגים של הציוד כולל גם תעבורה בין הציוד למשתמש טרם שלב ההזדהות (System -> Log/Monitoring -> User Access -> Settings and check [x] Unauthenticated Requests), מאחר וחלק מהתקיפות כנגד פגיעויות אלו מתבצעות בשלב זה.
10. הלוגים החשודים אמורים להיראות כך (דוגמאות - מודגש שם הקובץ המבוקש על ידי התוקף):

info - [x.x.x.x] - System()[][] - xxxx/xx/xx xx:xx:xx - VPN-Remote - Connection from IP x.x.x.x not authenticated yet (URL=

/dana-na/../dana/html5acc/guacamole/../../../../../../data/runtime/mtmp/lmdb/randomVal/data.mdb?/dana/html5acc/guacamole/)

/dana-na/../dana/html5acc/guacamole/../../../../../../data/runtime/mtmp/system?/dana/html5acc/guacamole/

/dana-na/../dana/html5acc/guacamole/../../../../../../etc/passwd?/dana/html5acc/guacamole/

11.[עדכון] ניתן לחפש בלוגים באמצעות ה- Regular Expression הבא:

\?.*/dana/html5acc/guacamole/

12.מומלץ לוודא כי לא נעשו שינויים בהגדרות להרצת סקריפטים על עמדות המשתמשים המתחברות לציוד ה- VPN. ניתן למצוא הגדרות אלו תחת users -> user roles -> VPN Tunneling -> Windows: Session start script.

3.13. מומלץ לבדוק בלוגים האם יש אינדיקציה למספר שינויים של כתובת ה-IP של משתמשים. שינוי כזה עשוי להיות לגיטימי, אם משתמש מורשה פועל משתי כתובות בו-זמנית, אולם אם מבוצע שינוי כזה הלוך ושוב בין 2 כתובות או יותר, ייתכן וזו אינדיקציה לכך שגם התוקף וגם המשתמש הלגיטימי מחוברים באותו session שפרטיו נגנבו על ידי התוקף. הלוג בעת שינוי כתובת ה-IP של session קיים נראה כך (דוגמה):

xxxx-xx-xx xx:xx:xx - PulseSecure - [1.2.3.4] DOMAIN\username - Remote address for user DOMAIN\username changed from 1.2.3.4 to 5.6.7.8

4.14. מומלץ לבצע בדיקה אחר לוגים המעידים על התחברות לממשקי האדמיניסטרציה של הציוד, ולנסות לאתר פעולות שלא בוצעו באופן לגיטימי (גם אם הן בוצעו לכאורה על ידי המנהלן - שכן ייתכן ופרטיו נגנבו):

1. פניות לנתיב /admin [עדכון] או /dana-admin/diag/diag.cgi עם שימוש בפרמטר =options ב- URL.
2. כניסה מכתובת IP בלתי מוכרת או קיום משתמשים מקומיים חדשים, במסך הבא:

Authentication -> Auth. Servers. -> users under “Administrators” and “System Local.”

15.[עדכון] מומלץ לבחון האם שונו הקבצים הבאים:

/etc/cloud_sshd_config

/.ssh/authorized_keys

המכילים את מפתחות ההצפנה עבור קישור ב- SSH לציוד ה- VPN.

16. [עדכון] מומלץ לבחון האם שונו חוקי ה- Firewall (IpTables) המותקן על ציוד ה- VPN. בפרט, האם הוגדרה גישה לציוד בפורט שהיה סגור קודם לכן.
17. [עדכון] מומלץ לבחון הלוגים לזיהוי פעילות חריגה, לדוגמה - שימוש בשמות משתמש לגישה מכתובות חו"ל, כאשר ידוע שהמשתמש בארץ, או גישה בשעות בלתי-סבירות.
18. במקרה של זיהוי אחד מהסימנים המחשידים המתוארים לעיל, מומלץ לשקול הצעדים הבאים:
    1. שחזור הגדרות הציוד מגיבוי שנלקח לפני מועד פרסום הפגיעות (אם קיים).
    2. איפוס סיסמאות גישה של כלל המשתמשים בציוד, כולל סיסמאות גישה בציוד ארגוני (כדוגמת Active Directory), באם הציוד מוגדר להזדהות באמצעותו.
    3. איפוס הציוד להגדרות היצרן והגדרתו מחדש.
    4. ארגונים רבים עושים שימוש בתעודה דיגיטלית אוניברסלית - לדוגמה *.example.com, עבור מספר שרתים בארגון, או בתעודה דיגיטלית זהה עבור פונקציה מסוימת, כגון מספר שרתי SSL VPN. לאור העובדה שחלק מהפגיעויות מאפשרות גישה ברמת Root לציוד, התוקף עלול להשיג גישה למפתחות הפרטיים של התעודה הדיגיטלית שבשימוש. במקרה של חשד ממשי למימוש בפועל של תקיפה כנגד הציוד, **מומלץ להחליף** את התעודה הדיגיטלית בכל השרתים שבהם נעשה שימוש בתעודה דיגיטלית זהה, מאחר והשגת המפתחות הפרטיים עלולה לאפשר לתוקף ביצוע מתקפת MITM (Man In The Middle) כנגד תעבורה מוצפנת המופנית לארגון.
19. המלצות היצרן להגדרה מאובטחת, ניתן למצוא בקישור הבא:

https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB29805/

לכל מידע נוסף ניתן לפנות אלינו. במידה שעלו ממצאים בבדיקתכם, נבקש לקבל היזון חוזר.

מקורות

1. https://www.gov.il/he/departments/publications/reports/vpn-urgent-alert-update
2. https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101
3. https://www.volexity.com/blog/2019/09/11/vulnerable-private-networks-corporate-vpns-exploited-in-the-wild/
4. https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/
5. https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities

שיתוף מידע עם הCERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כלשהו, במידה שהתגלה צורך כזה

בברכה,
CERT-IL