

התרעה דחופה: ציוד גישה מרחוק עלול

לאפשר תקיפת רשתות ארגוניות

28/02/2026

י"א אדר תשפ"ו

פעולות מידיות לביצוע:

- בטלו מיידית את האפשרות לגישה לממשק הניהול של הציוד מרשת האינטרנט (WAN).
- החליפו בהקדם האפשרי את כל סיסמאות המשתמשים, ובפרט המנהלנים, לסיסמה ארוכה ומורכבת וקשה לניחוש.
- חייבו שימוש בהזדהות חזקה (2FA) לכל גישה לציוד, בפרט של מנהלנים.
- שיקלו החלפת מפתחות ההצפנה בציוד.
- וודאו כי הציוד מעודכן לגרסה העדכנית ביותר שפורסמה על ידי היצרן, והקפידו על התקנה עיתית של עדכוני האבטחה בציוד.



שיתוף מידע עם מערך הסייבר 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.

[תקציר]

- לאור מצב החירום שהוכרז במשק, מערך הסייבר הלאומי מדגיש את הצורך לאבטח ציוד גישה מרחוק לרשתות הארגוניות כגון VPN, ZTNA וכד', וכן ציוד מסוג Firewall המשמש לבקרת תעבורה בין רשתות ארגוניות לרשת האינטרנט.

[פרטים]

- במקרים שונים בעבר, ציוד זה שימש כוקטור תקיפה מועדף על ידי תוקפים מדינתיים ואחרים, להשגת נגישות לרשתות ארגוניות.
- לאחרונה דווח על קמפיין שנעזר בכלי AI מוכרים לתקיפת כ-600 כתובות של ציוד Fortinet, בכ-55 מדינות ברחבי העולם, באמצעות נגישות לממשק הניהול של הציוד. במקביל דווחה עלייה של פי 7 בנסיונות תקיפה כנגד ציוד זה באמצעות שיטות Brute Force וניחוש סיסמאות גישה.
- **יודגש כי שיטות דומות עלולות לשמש לתקיפת ציוד מסוג דומה של יצרנים נוספים, והן אינן מוגבלות ליצרן מסוים.**

[דרכי התמודדות]

- בטלו מיידית את האפשרות לגישה לממשק הניהול של הציוד מרשת האינטרנט (WAN). אם נדרשת גישה ניהול מרחוק, הגבילו אותה לכתובות ספציפיות מוכרות בלבד.
- החליפו בהקדם האפשרי את כל סיסמאות המשתמשים, ובפרט המנהלנים, לסיסמה ארוכה ומורכבת וקשה לניחוש. בפרט יש לוודא שהציוד אינו משתמש בסיסמת ברירת מחדל כלשהי.
- אם הציוד תומך בכך, הגבילו לפרקי זמן גדלים והולכים ניסיונות לגישה אליו לאחר מספר ניסיונות הזדהות שגויים (3-5 לשיקולכם), למניעת תקיפה באמצעות ניחוש סיסמאות.
- חייבו שימוש בהזדהות חזקה (2FA) והצפנה מתאימה לכל גישה לציוד, בפרט של מנהלנים. הגבילו למינימום מספר המנהלנים המורשים לגשת לציוד מרחוק.
- וודאו כי אין משתמשים בלתי מוכרים המוגדרים בציוד.
- שיקלו החלפת מפתחות ההצפנה בציוד, בפרט אם יש חשד שהציוד הותקף בעבר או מותקף בהווה.
- וודאו כי הציוד מעודכן לגרסה העדכנית ביותר שפורסמה על ידי היצרן, והקפידו על התקנה עיתית של עדכוני האבטחה לציוד.

- וודאו כי הלוגים שמייצר הציווד נשמרים לתקופה סבירה (רצוי לפחות 3 חודשים, אך לכל הפחות חודש), בשרת ייעודי חיצוני לציווד. נטרו הציווד לאירועים חריגים (כגון הזדהות מנהלן מכתובת שאינה מוכרת ברשת האינטרנט, גישה בשעות חריגות וכו') ובחנו לוגים קיימים לזיהוי אנומליות.
- בחנו האפשרות להגביל הגישה לציווד ע"פ המיקום של הכתובת הפונה בעולם (Geo-Location). תשומת לב כי זהו פתרון חלקי מאחר ותוקפים מכירים שיטות לעקיפתו.
- אם הציווד תומך בהפעלת חוקי IPS, בחנו האפשרות להפעילם.
- ציווד שהוא EOL אינו מתוחזק עוד ולא מפרסמים עבורו עדכוני אבטחה, ולכן עלולות להיות בו פגיעויות רבות. מומלץ מאד לבחון חלופות לציווד מסוג זה ולהתקין בהקדם האפשרי.
- מומלץ להגדיר את הציווד כך שגם לאחר הזדהות מוצלחת, הגישה של המשתמשים לרשת הארגונית תהיה מוגבלת לשירותים, לפרוטוקולים ולפורטים הדרושים להם לצורך ביצוע עבודתם בלבד.
- אם ההזדהות לציווד מתבצעת באמצעות קישור למערכות ארגוניות כגון Active Directory, בחנו גם אותן לזיהוי הגדרות משתמשים חדשים ולא מוכרים או גישה חריגה לחשבונות מנהלנים, העלאת הרשאות וכד'.
- ראו המלצות נוספות בפרסום המערך https://www.gov.il/he/pages/alert_1886, סעיף "דרכי התמודדות", פסקה 5.
- משתמשי ציווד מתוצרת BeyondTrust, תשומת ליבכם להתרעת המערך בקישור https://www.gov.il/he/pages/alert_1962.
- בכל מקרה של פעילות חשודה המזוהה בציווד, מומלץ לפעול לפי הנוהל הארגוני עבור חשד לאירוע סייבר.