

13 באוגוסט 2023
כ"ו באב תשפ"ג
סימוכין: ב-ס-1588

התרעה חמורה: חשיפת בקרים לרשת האינטרנט מסכנת את פעילותם התקינה

תקציר



1. בקרים תעשייתיים (PLC) החשופים לגישה ישירה מרשת האינטרנט, מהווים סיכון לפעילות הבקר, מערכת הבקרה (ICS), והרשתות הארגוניות הנגישות מהבקר.
2. מטרת מסמך זה, הכרת תצורה נפוצה ופגיעה זו, וכיצד למנוע ניצולה על ידי תוקפים.

פרטים



1. בקרים תעשייתיים משמשים במגוון רחב של מגזרים כגון אנרגיה, תחבורה, חקלאות, ייצור וכד', לשליטה על מגוון רחב של מכונות ותהליכים.
2. בקרים אלו לא נועדו לרוב לחיבור ישיר לרשת האינטרנט, והם אינם מוגנים באמצעים השונים שבהם מחשבים מודרניים המחוברים לרשת נעזרים למניעת פגיעה.
3. מחזורי הרכש של ציוד זה הם ארוכים מאד, ולכן סבירות גבוהה שבקרים המותקנים בהווה במערכות שונות אינם מכילים אמצעים והגנות מודרניות כנגד תקיפת סייבר.
4. בעבר היו מספר מקרים ידועים בהם נוצלו בקרים הנגישים מרשת האינטרנט בישראל לתקיפה ומניפולציה, כולל על ידי תוקפים ממדינות אויב. לדוגמה:

- <https://www.haaretz.co.il/news/security/2022-09-05/ty-article/00000183-0dde-d968-abc7-4dffb5a0000>
- <https://www.ynet.co.il/articles/0,7340,L-5720969,00.html>
- <https://www.ynet.co.il/articles/0,7340,L-5740087,00.html>
- <https://news.walla.co.il/item/3571267>

ניתן לשותף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים

- <https://www.israelhayom.co.il/news/local/article/13917241>
- https://www.mako.co.il/news-digital/2021_q4/Article-381de635a4f7181026.htm
- <https://www.calcalist.co.il/calcalistech/article/skrhvq6y5>

5. הבקרים נתקפים לרוב בשל אחת מהאפשרויות הבאות:

1. השארת סיסמת ברירת המחדל של הבקר פעילה.
2. ניצול של פגיעות (מוכרת או שאינה מוכרת) בבקר. מטבעם של הבקרים, פגיעויות שכבר תוקנו בצידוד מחשוב מודרני, עדיין קיימות בבקרים שונים.
6. לאור האמור בסעיף הקודם, גם החלפת הסיסמה בבקר לסיסמה ארוכה ומורכבת, אינה ערובה כנגד תקיפת הבקר בהצלחה על ידי קבוצות תקיפה שונות.
7. תוקף המשיג אחיזה בבקר, עלול לשבש את פעולתו, או להרחיב את התקיפה הן אל רשת מערכת הבקרה עצמה ורכיבים נוספים בה, והן אל רשתות ארגוניות אחרות הנגישות מהבקר.

דרכי התמודדות



1. **מומלץ מאד** לוודא שבקרים אינם נגישים ישירות מרשת האינטרנט. מומלץ להגביל גישה לבקרים לכתובות ארגוניות ספציפיות על פי צורך בלבד. אם מסיבה עסקית נדרשת גישה לבקר מרשת האינטרנט, מומלץ לבצע משירות כגון VPN, עם הצפנה והזדהות חזקה מתאימה, ולהגביל באופן אקטיבי בבקר או ב-Router/Firewall רשת, את הגישה לכתובת זו בלבד.
2. מומלץ מאד לא לאפשר גישה חופשית לבקר מכל רשת האינטרנט, בין ברמת צפייה בלבד ובין בהרשאות מנהלן. מומלץ מאד לא לאפשר גישה חופשית לבקר החוצה מרשת הבקרה אל כל רשת האינטרנט או הרשת הארגונית. מומלץ להגביל הגישה לכתובות המחויבות לשם פעולה תקינה של הבקר.
3. ארגונים המשתמשים ברשת סלולרית לגישה לבקר, מומלץ מאד לבחון שימוש ב-APN להגדרת רשת פרטית בין הבקר לשאר המערכות הארגוניות, ללא גישה אל רשת האינטרנט וממנה.
4. מומלץ מאד לנהל את הבקר באמצעות פרוטוקולים מוצפנים בלבד.

ניתן לשתף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים

5. מומלץ מאד לבחון האפשרות לניהול הבקרים ממחשבים ייעודיים שזהו השימוש היחיד בהם, על מנת למנוע תקיפה של מחשבי הניהול ומהם מעבר לתקיפת הבקרים עצמם.
6. אם הבקר תומך במנגנוני הזדהות חזקה, מומלץ להפעילם.
7. אם קיימים בבקר מנגנוני רישום אירועים (לוגים) מומלץ להפעילם ולייצא את הלוגים למחשב ייעודי. מומלץ לבחון לוגים אלו באופן עיתי לזיהוי אנומליות או להיעזר במערכות ייעודיות כגון מערכות SIEM.
8. אם נדרשת תמיכת היצרן/הספק בבקר מרחוק, מומלץ להגבילה לכתובות הרלוונטיות ברשת היצרן. אם ניתן, יש לחייב יידוע של הארגון בפרטי הגישה הנדרשת, ואישורה טרם ביצועה בפועל.
9. מומלץ מאד להתעדכן באופן עיתי בפרסומי יצרן הבקרים, ולבחון ולהתקין את הגרסה העדכנית ביותר של תוכנת ההפעלה שלהם. יצרנים שונים מאפשרים רישום לרשימות דיוור על מנת לקבל עדכונים סדירים בנושאי אבטחה הנוגעים לבקרים.

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.

