פגיעות קריטית בבקרי Rockwell

מנוצלת בפועל על ידי תוקפים בעולם

09/03/2026
כ' אדר תשפ"ו

[תקציר]

- לאחרונה פורסם כי פגיעות קריטית ישנה משנת 2021 מנוצלת בפועל על ידי תוקפים בעולם לתקיפת בקרים מסדרות מסוימות של חברת Rockwell Automation.
- **לפגיעות עצמה לא הוצא עדכון על ידי החברה. מומלץ מאד לוודא שהבקרים אינם נגישים מרשת האינטרנט והגישה אליהם מהרשת הארגונית מוגבלת לכתובות ספציפיות.**

[פרטים]

- הפגיעות מזוהה כ-CVE-2021-22681.
- ציון הפגיעויות CVSS 10.0 (מקסימלי).
- ניצול הפגיעות עלול לאפשר לתוקף מרוחק, מעקף של מנגנון ההזדהות ושינוי של תצורת הבקר או של הקוד הפועל בו. פרטי הפגיעות בקישור מס' 2.
- רשימת המוצרים הפגיעים מופיעה בקישור מס' 9.
- מערך הסייבר הלאומי פרסם התרעה לגבי פגיעות זו כבר כשפורסמה בשנת 2021. ראו קישור מס' 1.

פעולות מידיות לביצוע:

- החברה לא הוציאה עדכון אבטחה לפגיעות זו, והמלצתה היא להפעיל את הבקרים ב-"Run Mode" (מתג המצב (Mode Switch) בבקר מועבר למצב ריצה) למניעת שינוי התצורה.
- מומלץ מאד לוודא כי הגישה לבקרים מוגבלת אך רק לכתובות הנדרשות לכך לצורך התהליך העסקי. **בפרט מומלץ לוודא כי אין גישה ישירה לבקרים מרשת האינטרנט.** אם מסיבה עסקית נדרשת גישה ישירה לרשת הבקרה מרשת האינטרנט, מומלץ לבצעה באמצעות שירות כגון VPN או ZTNA עם הצפנה והזדהות חזקה מתאימה.

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.

[דרכי התמודדות]

- החברה לא הוציאה עדכון אבטחה לפגיעות זו, והמלצתה היא להפעיל את הבקרים ב-"Run Mode" (מתג המצב (Mode Switch) בבקר מועבר למצב ריצה) למניעת שינוי התצורה. ראו קישור מס' 9.
- אם מסיבה כלשהי אין אפשרות להפעיל הבקרים באופן זה, היצרן ממליץ על מספר פעולות שיש לבצע על מנת להקטין הסיכון למימוש הפגיעות. ראו גם כן בקישור מס' 9.
- מומלץ מאד לוודא כי הגישה לבקרים מוגבלת אך רק לכתובות הנדרשות לכך לצורך התהליך העסקי. **בפרט מומלץ לוודא כי אין גישה ישירה לבקרים מרשת האינטרנט**. אם מסיבה עסקית נדרשת גישה ישירה לרשת הבקרה מרשת האינטרנט, מומלץ לבצעה באמצעות שירות כגון VPN או ZTNA עם הצפנה והזדהות חזקה מתאימה.
- המלצות מערך הסייבר הלאומי למניעת גישה ישירה מרשת האינטרנט למערכות ICS/SCADA/OT על כל רכיביהן, מופיעות בקישורים 4, 5.

[מקורות]

1. https://www.gov.il/he/pages/rockwell_1284
2. https://www.claroty.com/2021/02/25/blog-research-critical-authentication-bypass-in-rockwell-software/
3. https://us-cert.cisa.gov/ics/advisories/icsa-21-056-03
4. https://www.gov.il/he/pages/alert_1631
5. https://www.gov.il/he/pages/alert_1969
6. https://nvd.nist.gov/vuln/detail/cve-2021-22681
7. https://www.cisa.gov/news-events/alerts/2026/03/05/cisa-adds-five-known-exploited-vulnerabilities-catalog
8. https://www.cve.org/CVERecord?id=CVE-2021-22681
9. https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1550.html