

## פגיעויות במוצרי Ivanti

09/01/2025  
ט' טבת תשפ"ה

### פעולות מידיות לביצוע:

- בחינה ועדכון הציוד לגרסאות העדכניות ביותר בהקדם האפשרי.

### [תקציר]

- לאחרונה פורסמו 2 פגיעויות במוצרים שונים של חברת Ivanti.
- אחת הפגיעויות מנוצלת בפועל על ידי תוקפים בעולם ונצפו ניסיונות ניצול גם בישראל.

### [פרטים]

- הפגיעויות הן במוצרים Ivanti Connect Secure (ICS) , Ivanti Policy Secure (IPS) , Neurons for ZTA .
- הפגיעות החמורה יותר מזוהה כ-CVE-2025-0282, ציון CVSS 9.0, ועלולה לאפשר הרצת קוד מרחוק ללא צורך בהזדהות. **פגיעות זו מנוצלת בפועל בעולם.**
- פגיעות זו אינה קיימת בגרסאות 9.x של המוצר אך גרסאות אלו הן EOL.
- הפגיעות השניה עלולה לאפשר העלאת הרשאות למשתמש מזוהה.

### [דרכי התמודדות]

- מומלץ מאד לבחון ולעדכן בהקדם האפשרי את הציוד לגרסה העדכנית ביותר.
- פרטי הגרסאות העדכניות, ופרטים כיצד לנסות ולזהות תקיפה בקישורים 1,3. במקרה של זיהוי תקיפה המלצת היצרן היא לבצע Factory Reset.
- **תשומת לב כי בגרסאות 9.x ו-9.1Rx של המוצר הסתיימה התמיכה (EOL) בסוף חודש דצמבר 2024, ולא יפורסמו עדכוני אבטחה עבורו. מומלץ מאד לבחון ולעדכן הציוד לגרסה עדכנית ונתמכת בהקדם האפשרי.**

### [מקורות]

1. [https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en\\_US](https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US)
2. <https://www.ivanti.com/blog/security-update-ivanti-connect-secure-policy-secure-and-neurons-for-zta-gateways>
3. <https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day?e=48754805>

ניתן לשתף מידע המסווג TLP:|CLEAR עם כל קבוצת נמענים, לרבות ערוצים פומביים