

14 דצמבר 2020  
כ"ח כסלו תשפ"א  
סימוכין: ב-ס-1236  
[עדכון]  
15 דצמבר 2020  
כ"ט כסלו תשפ"א  
[עדכון]  
16 דצמבר 2020  
א' טבת תשפ"א  
[עדכון]  
20 דצמבר 2020  
ה' טבת תשפ"א

## [עדכון 3] התרעה דחופה: תוכנת SolarWinds Orion

### תקציר



לאחרונה פורסם כי חברת SolarWinds, יצרנית תוכנת Orion לניטור וניהול מערכות IT, הותקפה, ועדכוני התוכנה של מוצר זה נוצלו להדבקת לקוחות החברה במתווה שרשרת אספקה. [עדכון] החברה פרסמה גרסאות עדכניות למוצר. ראו סעיף "דרכי התמודדות" לפירוט הפעולות המומלצות לביצוע. [עדכון] מצורף קובץ מזהים עדכני.

### פרטים



1. [עדכון] לפי פרסומי החברה, הגרסאות שנוצלו לתקיפה הן 2019.4 HF 5, 2020.2 with no hotfix, ו-2020.2 HF 1. התוקפים שינו רכיבים שונים בקבצי העדכון.
2. חברת Fireeye פרסמה פרטים לגבי הפוגען המותקן במסגרת תקיפה זו, המכונה SUNBURST, וכן מידע לגבי האפשרויות לזיהויו. פורסמו חוקים עבור המנועים החינמיים YARA (המשמש לזיהוי קבצים זדוניים), Snort (המשמש לזיהוי תעבורת רשת זדונית), וה-AV החינמי ClamAV, ולמוצר מסחרי של החברה. פורסמו גם מזהי קבצים.
3. [עדכון] גם החברות מיקרוסופט ו-Volexity פרסמו מזהים עבור פוגען זה.

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

4. CISA, זרוע ה-DHS לאבטחת מידע וסייבר, הנחתה את כל הגופים הפדרליים המשתמשים במוצר זה, לנתקו מהרשת או לכבות את השרתים.
5. [עדכון] מערך הסייבר הלאומי יוסיף ויעדכן ככל שיתבררו פרטים נוספים.

**דרכי התמודדות**

1. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם במערכות הארגוניות.
2. [עדכון] לאור פרסומים כי לתוקף באירוע זה ייתכן והיו דרכים נוספות להשגת אחיזה ראשונית, מלבד תקיפת המוצר SolarWinds Orion, מומלץ גם לארגונים שאין ברשותם מוצר זה לנטר מזהים אלו.
3. [עדכון] רוב מזהי התעבורה (כתובות IP, שמות Domain) ממוקמים בתשתיות ענן. מומלץ לנטרם בלבד. מומלץ לחפשם בלוגים החל ממרץ 2020.
4. מומלץ מאד לבחון האם באפשרותכם לתפעל את מערכותיכם ללא מוצר זה עד להתבהרות התמונה המלאה, ולנתקו מהרשת או להשבית את השרתים. מומלץ לבצע הבדיקות המפורטות בסעיפים 3.2 ו-3.3 להלן.
5. אם אין באפשרותכם לבצע האמור לעיל, מומלץ לבצע הפעולות הבאות:
  1. לוודא באמצעות חוקי Firewall, כי השרתים בהם מותקן המוצר אינם יכולים לתקשר עם רשת האינטרנט, הן עבור תעבורה יוצאת והן עבור תעבורה נכנסת.
  2. לחפש בשרתים הרלוונטיים את מזהי הקבצים המצורפים להתרעה זו.
  3. לחפש בלוגים תעבורה המזוהה עם הפוגען, על פי המזהים המצורפים להתרעה זו. מומלץ לבצע חיפוש החל מחודש מרץ 2020.
  4. אם מערכותיכם הארגוניות תומכות בהגדרת החוקים שפורסמו על ידי Fireeye, מומלץ לבחנם ולהטמיעם במערכות אלו.
  5. מומלץ לוודא כי מערכותיכם תואמות את המלצות האבטחה של חברת SolarWinds למוצר. ראו קישור בסעיף "מקורות".
  6. מומלץ לעדכן מיידית את מערך הסייבר הלאומי בכל איתור של המזהים המצורפים במערכותיכם, וכן בכל אירוע חשוד הקשור למערכות SolarWinds בארגונכם.

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



6. [עדכון] החברה ממליצה למשתמשי הגרסאות 2020.2 with no hotfix, ו- 2020.2 HF 1, להתקין את גרסה 2020.2.1 HF2, ולמשתמשי גרסה 2019.4 HF 5 להתקין את גרסה 2019.4 HF 6. הגרסאות זמינות באתר החברה.

מקורות



1. <https://www.solarwinds.com/securityadvisory>
2. <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
3. <https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html>
4. <https://www.solarwinds.com/-/media/solarwinds/swdcv2/landing-pages/trust-center/resources/secure-configuration-in-the-orion-platform.ashx?rev=32603e0c87d84085b081f99a33fe5f4d&hash=62A998B9753957D82BC0F07005D38368>
5. <https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/>
6. <https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software>
7. [https://github.com/fireeye/sunburst\\_countermeasures](https://github.com/fireeye/sunburst_countermeasures)
8. [https://github.com/fireeye/sunburst\\_countermeasures/tree/main/indicator\\_release](https://github.com/fireeye/sunburst_countermeasures/tree/main/indicator_release)
9. [https://www.prologic.co.il/16\\_12\\_2020\\_-\\_%D7%A2%D7%93%D7%9B%D7%95%D7%9F\\_%D7%A1%D7%99%D7%99%D7%91%D7%A8\\_%D7%A9%D7%9C\\_solarwinds](https://www.prologic.co.il/16_12_2020_-_%D7%A2%D7%93%D7%9B%D7%95%D7%9F_%D7%A1%D7%99%D7%99%D7%91%D7%A8_%D7%A9%D7%9C_solarwinds)
10. <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>

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.



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