



27 בינואר 2021
י"ד בשבט תשפ"א
סימוכין: ב-ס-1270

פגיעות קריטיות בתוכנת Sudo

תקציר



1. תוכנת Sudo מאפשרת למנהלני מערכות הפעלה מבוססות Linux/UNIX להגדיר אילו משתמשים יכולים להריץ פקודות מסוימות בהרשאת Root.
2. לאחרונה דווח כי פגיעות בתוכנה מאפשרת לכל משתמש מקומי לקבל הרשאת Root, ללא צורך בהזדהות.
3. מומלץ לבחון ולהתקין את גרסת התוכנה העדכנית, בהקדם האפשרי.

פרטים



1. התוכנה פופולרית מאד ומותקנת ברוב המוחלט של הפצות Linux/UNIX, ובמערכת ההפעלה macOS.
2. הפגיעות ישנה, קיימת החל מיולי 2011, ומופיעה בגרסאות התוכנה 1.8.2 עד 1.8.31p2 (כולל) ובגרסאות התוכנה 1.9.0 עד 1.9.5p1 (כולל).
3. הפגיעות מזוהה כ-CVE-2021-3156. טרם נקבע ציון CVSS.
4. באתר הפרויקט מצוין כי הפגיעות ניתנת לניצול אם קיים קובץ בשם sudoers. קובץ זה קיים כברירת מחדל (בדרך כלל בנתיב /etc/sudoers).

דרכי התמודדות



1. מומלץ לבחון ולהתקין את גרסת התוכנה העדכנית – 1.9.5p2.

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

2. מומלץ לבדוק באתרי היצרנים של הפצות Linux/UNIX בשימוש ארגונכם, האם הופצה גרסה עדכנית לתוכנה. אם לא, ניתן להורידה גם מאתר הפרויקט.
3. סוגי ציוד רבים (לדוגמה – נתבים, מצלמות רשת, כונני רשת NAS וכד') עושים שימוש בגרסאות שונות של Linux. מומלץ לבדוק באתר היצרן האם הציוד מושפע מפגיעות זו והאם יצא עדכון לפגיעות.

מקורות

1. <https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit>
2. https://www.sudo.ws/alerts/unescape_overflow.html
3. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3156>
4. <https://www.sudo.ws/download.html>

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