

7 בנובמבר 2023
כ"ג בחשוון תשפ"ד
סימוכין: ב-ס-1657

פגיעויות בציוד QNAP

תקציר

1. לאחרונה פרסמה חברת QNAP מידע לגבי פגיעויות שונות במוצריה.
2. מומלץ מאד לבחון ולהתקין את גרסת התוכנה העדכנית ביותר על הציוד שברשותכם. מומלץ למנוע גישה לציוד מרשת האינטרנט.

פרטים

1. פורסמו 2 פגיעויות קריטיות (CVE-2023-23368, CVE-2023-23369). ציון CVSS 9.8 ו-9.0, בהתאמה.
2. הפגיעויות עלולות לאפשר לתוקף מרוחק לבצע פקודות מערכת הפעלה על הציוד ללא צורך בהזדהות.

דרכי התמודדות

1. מומלץ לעדכן את תוכנת הציוד לגרסה עדכנית על פי המפורט בקישורים 2, 3 בסעיף "מקורות" להלן.
2. מומלץ להגביל הגישה לציוד QNAP בפרט, וציוד NAS בכלל, לרשת הארגונית או הביתית, ובפרט למנוע גישה לציוד מרשת האינטרנט. אם מסיבה עסקית נדרשת גישה מסוג זה, מומלץ ליישמה באמצעות פתרון כגון VPN עם הזדהות חזקה והצפנה מתאימה.

מקורות

1. <https://www.qnap.com/en/security-advisories>
2. <https://www.qnap.com/en/security-advisory/qa-23-31>
3. <https://www.qnap.com/en/security-advisory/qa-23-35>

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

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