21 ביולי 2022
כ"ב בתמוז תשפ"ב
סימוכין: ב-ס-1473

פגיעויות במוצרי Atlassian

תקציר

1. חברת Atlassian פרסמה לאחרונה עדכוני אבטחה למוצריה.
2. הפגיעויות מוגדרות קריטיות ועלולות לאפשר למשתמש מרוחק לעקוף את מנגנון ההזדהות, או להזדהות באמצעות סיסמה קשיחה.
3. מומלץ לבחון את העדכונים הרלוונטיים לארגונכם ולהתקינם בהקדם האפשרי.

פרטים

1. 2 הפגיעויות הראשונות (CVE-2022-26136/26137) קיימות במוצרים הבאים:
   - Bamboo Server and Data Center
   - Bitbucket Server and Data Center
   - Confluence Server and Data Center
   - Crowd Server and Data Center
   - Fisheye and Crucible
   - Jira Server and Data Center
   - Jira Service Management Server and Data Center
2. הפגיעויות עלולות לאפשר מעקף של מנגנון הזדהות, תקיפה מסוג Cross Site Scripting, או מעקף של מנגנון Cross Origin Resource Sharing.
3. את הגרסאות בהן הפגיעויות קיימות ניתן למצוא בקישור הראשון בסעיף "מקורות" להלן.
4. פגיעות נוספת (CVE-2022-26138) קיימת במוצרים
   - Confluence Server

- Confluence Data center

5. הפגיעות קיימת אם מותקן בשרת הרכיב Questions for Confluence app.
6. הפגיעות עלולה לאפשר לתוקף מרוחק, שימוש בסיסמה קשיחה וקבלת הרשאות לצפייה ושינוי של כל העמודים הלא מוגבלים בשרת.
7. פירוט הגרסאות הפגיעות והדרכה ביצד לוודא אם השרת פגיע ניתן למצוא בקישור השני בסעיף "מקורות" להלן.

דרכי התמודדות

1. מומלץ לבחון והתקין בהקדם האפשרי את הגרסאות העדכניות שפרסמה החברה.
2. פירוט הגרסאות העדכניות ניתן למצוא בקישורים בסעיף "מקורות" להלן.

מקורות

1. https://confluence.atlassian.com/security/multiple-products-security-advisory-cve-2022-26136-cve-2022-26137-1141493031.html
2. https://confluence.atlassian.com/doc/questions-for-confluence-security-advisory-2022-07-20-1142446709.html