2023년 12월 Atlassian 취약점 긴급 공지

이 페이지는 2023년 12월 05일 Atlassian 제품에 대한 취약점을 긴급 공지하기 위하여 작성되었습니다.

개요

Atlassian Bitbucket, Confluence, Jira, Jira Service Management 취약점 발견

취약점 설명

아래 나열된 Atlassian 제품에서 고객에게 영향을 미치는 네개의 취약점이 발견되었습니다.
이 취약점 모두 CVSS 점수가 9.0 이상이므로 인스턴스를 보호하기 위해 즉각 조치를 취해야 합니다.

현재 사용하시는 버전을 확인하신 후 Atlassian 제품에 영향을 미치는 모든 중요한 보안 경고를 주의 깊게 검토하여 영향을 받는 버전과 지침을 확인하세요.

(1) 영향을 받는 제품

- **Bitbucket Data Center 및 Server**
    - CVE-2022-1471 - SnakeYAML 라이브러리 원격 코드 실행(RCE) 취약점

- **Confluence Data Center 및 Server**
    - CVE 2023 22522 - Confluence Data Center 및 Server RCE 취약점
    - CVE 2022 1471 - SnakeYAML 라이브러리 원격 코드 실행(RCE) 취약점
    - CVE 2023 22524 - Atlassian Companion App for MacOS (이전 사용자 포함) RCE 취약점

- **Jira Service Management Cloud, Data Center 및 Server**
    - CVE 2023 22523 - Assets Discovery app RCE 취약점
    - CVE 2022 1471 - SnakeYAML 라이브러리 원격 코드 실행(RCE) 취약점 (Data Center 및 Server만 해당)

- **Jira Software 및 Jira Core Data Center 및 Server, Automation for Jira apps**
    - CVE-2022-1471 - SnakeYAML library RCE vulnerability impacts multiple products

(2) 해결 방법

- 제품을 안내된 최신 버전 또는 수정 버전으로 업데이트 바랍니다.
- 즉시 업데이트할 수 없는 경우 연결된 페이지의 방법을 따라 임시 조치를 취하여 외부의 공격을 완화시킬 수 있습니다.

하기 링크를 클릭하시면 취약점과 관련하여 커브 안내 페이지로 이동합니다.

- Atlassian 공통 보안 취약점 CVE-2022-1471
- Confluence 보안 권고 CVE-2023-22522