Bitbucket Server and Data Center Security Advisory 2022-11-16

요약	CVE-2022-43781 - Command Injection Vulnerability
권고일	2022년 11월 16일
제품	• Bitbucket Server • Bitbucket Data Center
CVE ID(s)	CVE-2022-43781

취약점 요약

이 권고는 Bitbucket Server 및 Data Center 버전 7.0.0에 도입된 Critical 심각도의 보안 취약점을 공개합니다.
이 취약점의 영향을 받는 버전은 다음과 같습니다.

- Bitbucket Data Center 및 Server 7.0에서 7.21 까지의 버전
- Bitbucket Data Center 및 Server 8.0 에서 8.4까지 (`mesh.enabled` 가 `bitbucket.properties`에서 false로 설정된 경우)

Bitbucket Server 및 Data Center에는 환경 변수를 사용하는 커맨드 인젝션 취약성이 있습니다.
사용자 이름을 제어할 수 있는 권한이 있는 공격자는 코드를 실행하는 이 이슈를 악용하고 시스템에서 코드를 실행할 수 있습니다.

이 이슈는 다음에서 추적 가능합니다.

BSERV-13522 - Critical severity command injection vulnerability - CVE-2022-43781

Atlassian Cloud는 영향을 받지않습니다.

심각도

Atlassian은 Atlassian 심각도 수준에 게시된 척도에 따라 이 취약성의 심각도 수준을 **Critical**로 평가합니다.
척도를 사용하여 심각도를 위험, 높음, 중간 또는 낮음으로 순위를 매길 수 있습니다.

영향받는 버전

7.0 버전에서 7.21 버전까지 의 모든 버전의 Bitbucket Server 및 Data Center 가 이 취약점의 영향을 받습니다.
Bitbucket Server 및 Data Center 의 8.0~8.4 버전은 `mesh.enabled=false` 가 `bitbucket.properties` 에 설정된 경우 이 취약점의 영향을 받습니다.

수정된 버전

제품	수정 버전

Bitbucket Server 및 Data Center	• 7.6.19 또는 최신 버전 • 7.17.12 또는 최신 버전 • 7.21.6 또는 최신 버전 • 8.0.5 또는 최신 버전 • 8.1.5 또는 최신 버전 • 8.2.4 또는 최신 버전 • 8.3.3 또는 최신 버전 • 8.4.2 또는 최신 버전 • 8.5.0 또는 최신 버전

권고 사항

Atlassian은 영향을 받는 각 버전에 대하여 수정 버전(또는 이후 버전) 중 하나로 업그레이드할 것을 권장합니다.
최신 버전의 Bitbucket Server 및 Data Center에 대한 전체 설명은 릴리스 정보 를 참조하세요. 다운로드 센터에서 최신 버전의 Bitbucket을 다운로드할 수 있습니다.

임시 방법

Bitbucket 인스턴스를 업그레이드할 수 없는 경우 "공개 가입"을 비활성화하는 임시 방법이 있습니다.
공개 가입을 비활성화하면 공격 벡터가 인증되지 않은 공격에서 인증된 공격으로 변경되어 악용될 위험성이 줄어듭니다.
이 설정을 비활성화하려면 **Administration** > **Authentication**으로 이동하여 **Allow public sign up** 확인란을 선택 취소합니다.

ADMIN 또는 SYS_ADMIN 인증된 사용자는 공개 등록이 비활성화된 경우에도 취약성을 악용할 수 있습니다.
때문에 이러한 조치는 임시 단계로 취급되어야 하며 가능한 빨리 수정 버전으로 업그레이드하는 것을 권장드립니다.

PostgreSQL을 실행하는 Bitbucket Server 및 Data Center 인스턴스는 영향을 받지 않습니다.