Crowd Security Advisory (November 2022)

요약	CVE-2022-43782 - Critical security misconfiguration vulnerability
권고일	2022년 11월 16일
제품	Crowd Server 및 Data Center
CVE ID(s)	CVE-2022-43782

https://confluence.atlassian.com/crowd/crowd-security-advisory-november-2022-1168866129.html

취약점 요약

이 권고는 Crowd 3.0.0에서 도입된 Critical 심각도의 보안 설정 오류 취약점을 공개합니다.
3.0.0 버전 이후 출시된 모든 버전이 영향을 받지만 다음 조건이 모두 충족되는 경우에만 해당됩니다.

- 이 취약점은 영향을 받는 버전의 **새로 설치한 것**과 관련이 있습니다. 이전 버전(예: 버전 2.9.1)에서 버전 3.0.0 이상으로 업그레이드한 경우 인스턴스는 영향을 받지 않습니다.
    - 새로 설치한 것은 다운로드 페이지에서 원래 다운로드한 것과 동일한 버전의 Crowd 인스턴스로 정의되며, 이후 업그레이드 않았습니다.
- IP 주소가 Crowd 애플리케이션의 Remote Address 구성에 추가되었습니다(버전3.0.0 이후 버전에서는 기본적으로 없음).

이 취약점을 통해 허용 목록의 IP로 연결된 공격자는 암호 확인을 우회하여 Crowd 애플리케이션으로 인증할 수 있습니다.
이를 통해 공격자는 Crowd의 REST API에서 *usermanagement* 경로 아래에 있는 특권을 가진 엔드포인트를 호출할 수 있습니다.
위에서 설명한 바와 같이 Remote Addresses 구성에서 Crowd 애플리케이션의 허용 목록에 명시된 IP에 의해서만 악용될 수 있습니다.
이 취약점을 해결하기휘애 아래의 '수정 버전'에 나열된 수정 버전 중 하나로 인스턴스를 업그레이드할 것을 권장합니다.

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

Crowd 3.0.0 버전 이후의 모든 버전이 영향을 받습니다.

- Crowd 3.0.0 - Crowd 3.7.2
- Crowd 4.0.0 - Crowd 4.4.3
- Crowd 5.0.0 - Crowd 5.0.2

앞서 언급했듯이 새로 설치한 경우에만 취약합니다. 예를 들어 버전 2.9.1에서 3.0.0으로 업그레이드한 경우 인스턴스는 영향을 받지않습니다.
그러나 이 경우 버전 2.9.1에 있던 기존 remote addresses는 버전 3.0.0을 실행하는 인스턴스로 전달됩니다.
이는 Crowd 애플리케이션의 Remote Addresses 구성에서도 제거할 수 있습니다.

사용자 관리를 위해 Embedded Crowd에 의존하는 기타 Atlassian Data Center 및 Server 제품은 영향을 받지 않습니다.

수정 버전

Crowd 버전	Bug fix release
Crowd 5.0	5.0.3 또는 그 이후 버전
Crowd 4.0	4.4.4 또는 그 이후 버전
Crowd 3.0	이 버전은 더 이상 사용되지 않으므로 수정할 수 없습니다. Crowd 4.4.4 또는 5.0.3으로 업그레이드하세요.

권고 사항

Atlassian은 상기 '수정 버전' 중 하나로 인스턴스를 업그레이드하는 것을 권고합니다. 최신 버전의 Crowd에 대한 전체 설명은 릴리스 정보를 참조하세요.
다운로드 센터에서 Crowd의 최신 버전을 다운로드할 수 있습니다.

인스턴스가 손상되었는지 확인

다음 리소스를 사용하여 인스턴스가 손상되었는지 확인할 수 있습니다.

Access Logs

Crowd는 기본적으로 액세스 로그를 제공하지 않습니다. 이 정보는 잠재적인 공격이 발생하기 전에 액세스 로그를 구성한 경우에만 유효합니다.
액세스 로그를 구성한 경우 Crowd에 연결된 다른 제품에서 발생하지 않는 *usermanagement* 경로에 대한 호출 범위를 좁힐 수 있어야합니다.
Access logging for Crowd

Audit log(Data Center인 경우에만 해당)

Crowd audit log에서 Crowd로 수행된 작업을 검색할 수 있습니다.
Browsing the audit log.

임시 방법

취약점을 해결하기위해서는 영향 받는 버전을 수정된 버전으로 업그레이드해야합니다. 현재 Crowd 업그레이드를 할 수 없는 경우 아래의 임시 방법을 사용할 수 있습니다.

Remote Address 삭제

Crowd 제품에서 **crowd appliaction**의 Remote Address를 제거하거나 유효성을 검사하여 문제를 일시적으로 완화할 수 있습니다.(사용자가 추가한 다른 application들은 제외)

> ⚠ 제거 전 현재 등록된 정보에 대해서 기록을 남겨 복원 할 수 있도록 해주세요.

Remote Address 삭제 방법은 다음과 같습니다.

1. Crowd Administration Console 로그인
2. 네비게이션 바 상단에 **Applictions** 클릭
3. Application Browser에서 **crowd application** 선택
4. **View Application** 화면에서 **Remote Addresses** 탭 클릭
5. Remore Address를 삭제

표시될 수 있는 Remote Address에 대한 정보는 다음과 같습니다.

- Crowd 3.0.0 버전 또는 그 이후 버전의 새로운 설치는 기본적으로 remote address가 없습니다.
- 3.0.0 버전 보다 이전 버전이거나 그러한 버전에서 업그레이드한 인스턴스의 경우 기본적으로 많은 원격 주소가 있을수 있습니다.
  이러한 원격 주소는 버전 3.0.0 이후에는 사용되지 않으므로 제거할 수 있지만 취약성 완화에는 영향을 주지 않습니다.

비밀번호 변경

더불어, remote address를 제거할 수 없는 경우 **crowd application**의 비밀 번호를 더 강력한 것으로 변경할 수 있습니다.

비밀번호 변경하는 방법은 다음과 같습니다.

1. Crowd Administration Console 로그인
2. 네비게이션 바 상단에 **Applictions** 클릭
3. Application Browser에서 **crowd application** 선택
4. **Details** 탭에서 **Change password** 선택