

Confluence 보안 취약성 공지

이 문서는 Confluence 관련 보안 취약성 공지와 조치사항에 대한 정보를 공유하기 위해 작성되었습니다.

- [Confluence Security Advisory - 2021-08-25](#)

개요

최근 Atlassian Confluence 제품의 취약점을 이용한 악용사례가 있어 최신 버전으로 업데이트할 것을 권고 합니다.

※ Confluence : 조직 내 프로젝트 관리를 위한 협업 솔루션

취약점

Confluence Server 및 Data Center에서 OGNL 인젝션으로 인해 발생하는 원격코드실행 취약점(CVE-2021-26084)

*영향: 승인되지 않은 사용자가 Confluence 서버에 임의의 코드를 실행할 수 있습니다.

[더보기](#)

영향 받는 제품 및 해결방안

1) 긴급 패치 적용

현재 최신 버전으로 업그레이드 진행이 어려운 경우 수분 내에 적용할 수 있습니다.

[긴급 패치 적용방법](#)

2) 업그레이드

Atlassian 홈페이지의 "download centre" 항목을 참고하여 최신 버전으로 업그레이드하시기 바랍니다.

제품명	영향받는 버전	취약점 해결 버전
Confluence Server 및 Data Center	6.12.23 이전 버전	6.13.23 버전
	6.14.0 ~ 7.4.X 버전	7.4.11 버전
	7.5.0 ~ 7.11.X 버전	7.11.6 버전
	7.12.X 버전	7.12.5, 7.13.0 버전
*Confluence Cloud는 영향 받지 않습니다.		

[다운로드 바로가기](#)