

Logback 보안 업데이트 권고(CVE-2021-42550)

이 문서는 Logback 에서 발생하는 취약점에 대해 공유하기 위해 작성되었다.

※ CVE-2021-42550은 사전 요구 사항으로 로그백의 구성 파일에 대한 쓰기 액세스 권한이 필요함. 따라서 Log4J 2(log4Shell) 취약점과 CVE-2021-42550은 서로 다른 심각도 수준임을 참고.

- [Logback 보안 업데이트 권고](#)
 - [보안 취약 코드](#)
 - 주요 내용 및 영향 받는 버전, 공통적인 대응방안
 - [추가 참고 URL](#)

Logback 보안 업데이트 권고

보안 취약 코드

- **CVE-2021-42550**
 - Logback에서 발생하는 원격코드실행 취약점
 - [CVE - CVE-2021-42550 \(mitre.org\)](#)

주요 내용 및 영향 받는 버전, 공통적인 대응방안

KISA 보안공지 - 'Logback 보안 업데이트 권고' 항목 참고

- https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=36396

추가 참고 URL

- **Logback News**
 - <http://logback.qos.ch/news.html>
 - **제조사별 현황**
 - [log4shell/software at main · NCSC-NL/log4shell · GitHub](#)
-