WordPress 원격코드 실행 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.21

□ 개요
o WordPress社는 자사 제품의 취약점을 해결한 보안 업데이트 발표 [1]
o 영향 받는 버전을 사용중인 이용자는 최신버전으로 업데이트 권고

□ 설명
o WordPress에서 사용자의 입력값에 대한 검증 기능이 미흡하여, Post Meta를 이용하여 악성코드가 담긴 PHP를 실행하여 발생하는 원격코드 실행 취약점(CVE-2019-8942)
※ Post Meta : WordPress에 이미지를 업로드할 때, 해당 이미지에 대한 내부 참조 정보로, DB에 Post Meta 항목으로 저장됨

□ 영향을 받는 제품
o WordPress
- 5.0.1 이전 버전(단, 4.9.9버전은 영향받지 않음)

□ 해결 방안
o 4.9.9 또는 5.0.1 이상 버전으로 업데이트
- 대쉬보드(알림판) - 업데이트 - "Update Now" 클릭

□ 기타 문의사항
o 한국인터넷진흥원 인터넷침해대응센터: 국번없이 118

[참고사이트]
[1] https://nvd.nist.gov/vuln/detail/CVE-2019-8942

주소 : 서울특별시 서초구 서초대로 255 고덕빌딩 2층 [06595]
전화 : 02-2105-4400 (영업문의 1, 보안관제문의 2, 기술문의 3)
팩스 : 02-2105-4456
영업문의 : sales@eosec.co.kr, 보안관제 및 기술문의 : tech@eosec.co.kr