

홈페이지 운영자를 위한

PHP2Shell 보안 취약점 FAQ

기준일
2026. 10. 25.

지금 해야 할 3가지

STEP 1

PHP 사용 여부 확인

제작·호스팅 업체에 PHP 버전과 조치 여부 문의

STEP 2

최신 버전 업데이트

업데이트 → 재시작 → 추가 보안 설정

STEP 3

이상징후 확인

비밀번호 교체·흔적 점검
이상하면 118 신고

1단계 기본 질문

Q1 ~ Q8



Q1 내부 업무망에도 PHP가 있나요?

있습니다 인트라넷·ERP·그룹웨어, VPN·방화벽 관리 화면에도 쓰입니다. 내부망 시스템도 함께 점검하세요.



Q2 우리 홈페이지도 해당되나요?

- 워드프레스·그누보드 등 PHP 기반이면 해당됩니다.
- 업체에 "PHP 버전과 조치 여부"를 묻는 것이 가장 빠릅니다.



Q3 무료로 확인하는 방법은요?

보안기업 점검 사이트에 주소를 넣으면 PHP 버전을 알려 줍니다.

스틸리언
stealien.com/php2shell

엔키화이트햇
vuln.offen.im

티오리
phpguard.io

파이오링크
piolink.com/kr/php2shell

※ 사이트별 결과가 다를 수 있으니 운영자가 직접 확인하세요.



Q4 조치는 누가 하나요?

- 호스팅·제작 업체가 조치합니다. (직접 조치도 가능)
- 운영자는 업체에 요청하고 조치 결과를 회신받아 관리하세요.



Q5 업데이트하면 끝인가요?

아닙니다 업데이트 후 반드시 재시작해야 적용되며, 이후에도 지속적인 점검이 필요합니다.



Q6 당장 업데이트가 어렵다면요?

- 보안 설정 → 흔적 점검 → 비밀번호 교체
- 보호나라 공지를 참고하세요.
 - 이마저 어렵다면 홈페이지 일시 중단을 검토하세요.



Q7 중소기업·소상공인 지원은요?

- 지역정보보호지원센터(전국 16곳, risc.kisa.or.kr) 상담
- 보호나라 무료 홈페이지 취약점 점검 활용
- 패치 적용은 제작·호스팅·보안업체에 문의하세요.



Q8 해킹이 의심되면요?

- 화면 변조, 모르는 파일·계정이 보이면
- 서버는 끄지 말고 외부 접속만 차단 (랜선 분리 등)
 - 그다음 118 또는 보호나라에 신고하세요.

안전한 PHP 버전 (이상)

8.5.12

8.4.27

8.3.36

8.2.35

8.2는 12월 31일 지원 종료 → 8.3 이상 권장

118

해킹 의심 시 즉시 신고

KISA 인터넷침해대응센터
상담·신고 (국번 없이)

2단계 상세 질문

확인 → 조치 → 업데이트가 어려울 때 → 해킹 의심 시

1 확인하기

Q1·Q2·Q3 관련



Q9 로그인 기능이 있으면 괜찮지 않나요?

아닙니다 로그인 이전 단계에서도 공격 가능합니다.
버전 정보 노출 차단: `expose_php = Off` (php.ini)



Q10 취약점 3건, 따로 조치하나요?

10.21 공지 CVE-2026-109618, -109619 → 업데이트

10.24 공지 CVE-2026-115560
→ 보안 업데이트로 패치, 그 전까지 추가 보안 설정



Q11·12 안전한 버전과 확인 방법은요?

8.3 이상 권장(버전 기준은 앞면 하단), 확인은 앞면 Q3 점검 사이트를 이용하세요.



Q13 홈페이지 외에 확인할 대상은요?

관리자 페이지, 안 쓰는 옛 홈페이지, PHP 탑재 장비도 확인하세요. 안 쓰는 홈페이지는 닫고, 장비는 제조사 공지를 확인하세요.

2 조치하기

Q4·Q5 관련



Q14 업체에 뭐라고 요청하나요?

"KISA 보호나라 공지를 참고해 PHP 취약점을 조치하고, **10월 20일 이후** 흔적 점검 결과를 알려 주세요."



Q15 업체가 "조치 완료"라면?

✓ 적용 버전 ✓ 재시작 ✓ 보안 설정

호스팅사 공지라면 우리 버전이 대상인지도 확인하세요.



Q16 제작 업체가 없어졌다면요?

새 업체에 요청해 조치하고, 유지보수 계약으로 주기적으로 관리하세요.



Q17 업데이트 시 장애는 없나요?

생길 수 있습니다 반드시 백업 후 사전 테스트를 진행하세요.



Q18 인증정보도 교체해야 하나요?

교체 권장: 인터넷에 연결된 DB 비밀번호, 외부 서비스 연동 키, 관리자 계정 비밀번호

3 업데이트가 어려울 때

Q6 관련



Q19 웹방화벽이 있으면 안전한가요?

아닙니다 공격 일부만 막을 뿐, 완전한 해결은 업데이트뿐입니다.



Q20 8.1 이하라 업데이트가 없다는데요?

업체에 **8.3 이상 전환**을 요청하고, 전환 전까지 서비스 중지 등 임시 조치를 하세요. 중지가 어렵다면 화면 변조·파일·계정 모니터링을 강화하세요.

4 해킹이 의심될 때

Q8 관련



Q21 취약 버전이면 이미 해킹된 건가요?

꼭 그렇지는 않습니다

단, 심어진 악성 파일은 업데이트로 지워지지 않으니 KISA·보안업체 점검이나 보호나라 '해킹진단도구'로 점검하세요.



Q22 왜 서버를 끄면 안 되나요?

공격 흔적이 사라져 피해 범위를 알 수 없습니다. (업데이트 후 재시작과는 별개)



Q23 고객정보가 유출됐다면요?

보호나라 침해사고 신고 + 개인정보보호위원회 유출 신고. 먼저 118로 문의하세요.

해킹 의심·침해사고 신고

118

국번 없이

보안공지·신고·해킹진단도구

KISA 보호나라

boho.or.kr

중소기업·소상공인 보안 상담

지역정보보호지원센터

전국 16곳 · risc.kisa.or.kr