과학기술정보통신부 보도자료 대체불가 대한민국

보도시점 2026. 10. 22.(목) 즉시 배포

과기정통부, 웹사이트 개발 언어 'PHP' 보안 취약점 관련 긴급 보안 업데이트 및 기술적 조치 당부

- 웹사이트 운영 기업·기관은 즉시 업데이트, 구버전은 상위 버전 전환 및 침해 여부 점검 필요
- 민간 분야 사이버위기 경보 '관심'에서 '주의'로 상향 조정

과학기술정보통신부(부총리 겸 과학기술정보통신부 장관 배경훈, 이하 '과기정통부')와 한국인터넷진흥원(원장 이상중, 이하 'KISA')은 전 세계 웹사이트 제작에 널리 쓰이는 프로그래밍 언어 **'PHP'에서 심각한 보안 취약점 2건이 공개**되었다고 밝혔다. 이에 따라 PHP를 이용한 홈페이지를 운영하는 국내 기업·기관에 **보안 업데이트를 즉시 적용할 것을 당부**하였다.

PHP는 홈페이지, 온라인 쇼핑몰, 게시판, 관리자 페이지 등 **다양한 웹 서비스를 만드는 데 사용되는 프로그래밍 언어**로, 워드프레스·그누보드 등 국내에서 많이 쓰이는 홈페이지 제작 도구도 PHP를 기반으로 동작한다.

이번에 발견된 취약점은 공격자가 아이디·비밀번호 없이 인터넷을 통해 특수하게 조작된 요청을 보내는 것으로서 **서버에 원하는 명령을 실행**할 수 있어 **위험도가 높다**. 공격에 성공하면 해커가 서버에 원격조종 파일(webshell)을 몰래 설치하거나, 고객 정보 유출, 홈페이지 변조·마비 등 중대한 피해로 이어질 수 있다.

특히, 이번 취약점은 개별 홈페이지의 프로그램이 아닌 **PHP 자체의 보안 취약점**으로 홈페이지 프로그램을 안전하게 만들었음에도 영향을 받을 수 있다.

이에 유럽연합 사이버보안기관(CERT-EU), 영국·네덜란드·독일 등 **주요국 사이버보안 기관**도 **이번 취약점을 '치명적' 등급으로 평가**하고, 즉시 업데이트하되 당장 **업데이트가 어려운 시스템**은 **인터넷에서 분리**하거나 **일시 중단할 것을 권고**하고 있다.

PHP 개발팀은 10월 21일(현지시각) 취약점을 해결한 **보안 업데이트를 배포**했으며, KISA는 같은 날 보호나라 누리집*을 통해 **보안 업데이트 권고문을 게시**했다.

* KISA 보호나라 : www.boho.or.kr (알림마당 → 보안공지 → 'PHP 제품 보안 업데이트 권고')

PHP를 사용하는 기업·기관은 운영 중인 모든 홈페이지와 시스템의 **PHP 버전을 확인**하고, **최신 버전*으로 즉시 업데이트**해야 한다. 업데이트 후에는 반드시 **웹 서비스를 재시작**해야 보안 조치가 적용된다.

* PHP 8.5.12, 8.4.27, 8.3.36, 8.2.35 이상

특히 **PHP 8.1 이하 구버전**은 공식 업데이트가 제공되지 않으므로, 지원되는 **상위 버전으로 전환**해야 한다. 오래전에 만들어 두고 관리하지 않는 홈페이지, 외주로 제작한 쇼핑몰, 장비 관리 화면 등에도 PHP가 사용되고 있을 수 있어 꼼꼼한 확인이 필요하다.

아울러 취약점 정보가 이미 유출된 만큼, 업데이트를 마친 서버라도 **이상 접속 기록**이나 **원격조종 파일**(webshell) **설치 여부 등 침해 흔적을 점검**하고, 피해가 의심될 경우 즉시 KISA에 신고*해야 한다.

* 상세 내용은 보호나라 누리집(알림마당 – 보안공지) 참고

호스팅 업체를 이용해 홈페이지를 운영하는 소상공인 등은 이용 중인 **호스팅 업체에 보안 업데이트 적용 여부를 확인**하면 된다. **일반 국민은 직접 조치할 사항은 없으나, 평소와 같이 백신 설치, 최신 보안 업데이트 등 기본적인 보안 수칙을 지키는 것이 좋다.**

또한, 인터넷에 '공격 시험 코드(PoC)'라며 유포되는 파일 중에는 악성코드가 숨겨진 가짜가 많으므로, **출처가 불분명한 코드는 내려받거나 실행하지 말아야 한다.**

과기정통부(KISA)는 CISO 신고기업, 주요정보통신기반시설, 정보보호 관리체계(ISMS) 인증기업, 웹호스팅사, 인터넷데이터센터(IDC), 사이버위협 정보 공유(C-TAS) 회원사 등에 **관련 내용을 긴급 전파**하였으며, 국내외 보안업계와 협력해 **공격 동향을 지속적으로 모니터링**하고 있다.

※ CISO 신고기업 약 2.8만개, 주요정보통신기반시설 111개, 정보보호 관리체계(ISMS) 인증기업 1,068개 C-TAS 회원사 5,900개, 웹 호스팅사, 인터넷데이터센터 등 주요기업 688개

과기정통부는 KISA와의 위기평가 회의를 거쳐, PHP 취약점으로 인한 대규모 해킹 가능성에 대한 경각심을 높이고 선제적으로 대응하기 위해 10. 22일 12:00부로 민간 분야 사이버위기 '주의' 경보를 발령한다고 밝혔다.

※ 민간분야 사이버위기 경보단계는 '관심→**주의**→경계→심각'으로 구분

'주의' 경보 발령 시, 피해가 발생한 경우에 신속히 대응할 수 있도록 침해대응 인력을 증원하고, 비상출동조를 상시 대기시키는 등 비상대응 체계를 가동하게 된다.

과학기술정보통신부 배경훈 부총리는 "이번 PHP 취약점은 **국내 수많은 홈페이지에 영향**을 줄 수 있고, 공격코드까지 이미 공개된 만큼 **매우 시급한 대응이 필요**하다"며, "기업 관점에서는 기존의 수동 점검 후 수일 내 패치라는 통상적인 취약점 관리 주기(SLA)로는 공격을 방어할 수 없으며, **인터넷 접점 자산에 대한 즉각적인 차단** 및 웹방화벽(WAF) 룰셋 선제 적용 같은 **자동화된 대응 체계가 필수**적"이라고 언급했다. 마지막으로 전 부처가 원팀으로 대응해야할 엄중한 상황으로 각 부처와 협력하여 중소기업 대상 보안점검 및 조치 요청을 논의할 예정이라고 덧붙였다.

담당 부서	정보보호네트워크정책관 사이버침해대응과	책임자	과 장	김단호 (044-202-6460)
		담당자	사무관	장민영 (044-202-6465)
유관 기관	한국인터넷진흥원 디지털위협대응본부	책임자	본부장	박용규 (02-405-4100)
		담당자	단 장	심재홍 (02-405-4700)

대체불가 대한민국 내일을 만드는 과학기술 내삶을 채우는 디지털·AI 대한민국 정책브리핑 OPEN 공공누리 공공저작물 자유이용허락 OPEN

붙임 **PHP 보안취약점 관련 기업 보안 대응 수칙**

PHP 보안취약점(PHP2Shell) 관련 기업 보안 대응 수칙

□ 개요

o PHP에서 로그인 없이 외부에서 서버에 원하는 명령을 실행할 수 있는 치명적 보안 취약점(CVE-2026-109618, CVE-2026-109619, CVSS 9.2) 발견 [1][2][3][5]

o 보안 업데이트 배포 전 취약점 정보가 유출되었고 해외 보안업체를 중심으로 공격 시도가 보고되고 있으며, 공격에 성공하면 원격조종 파일(웹셸) 설치, 고객정보 유출, 홈페이지 변조, 내부망 침투 등 가능

o PHP를 사용하는 기업은 아래 대응 수칙에 따라 즉시 조치할 것을 권고

※ 호스팅 업체나 장비·솔루션 제조사가 PHP를 관리하는 경우, 해당 업체에 아래 조치의 적용 여부를 확인하고 요청

□ 기업 보안 대응 수칙

1. 운영 중인 PHP 사용 현황 확인

o 인터넷에 공개된 모든 홈페이지와 시스템의 PHP 사용 여부와 버전 확인

- 외주 제작 사이트, 오래전에 만들어 두고 관리하지 않는 사이트, 이벤트·테스트 서버, 관리자 페이지 포함
- 자산 관리 목록에만 의존하지 말고, 실제 동작 중인 서버를 기준으로 확인

o PHP가 내장된 장비·솔루션(네트워크 장비 관리 화면, PHP가 포함된 윈도우용 설치 패키지 등)과 외부에서 받아 쓰는 컨테이너 이미지(도커 등)도 별도 확인 [4]

2. 최신 버전 업데이트 및 재시작

o 해결 버전: PHP 8.5.12, 8.4.27, 8.3.36, 8.2.35 이상 (리눅스 배포판·제조사 제공 업데이트 포함)

o 인터넷에 공개된 서버부터 우선 조치

o 업데이트 후 PHP를 실행하는 모든 웹 서비스(PHP-FPM, Apache mod_php, php-cgi, FrankenPHP, LiteSpeed 등)를 반드시 재시작

- 재시작하지 않으면 메모리에 남은 이전 버전이 계속 동작해 여전히 취약
- 컨테이너 환경은 신규 이미지 재배포

o 업데이트 후 웹 서비스가 실제로 사용하는 PHP의 버전이 바뀌었는지 확인

※ 명령어(php -v)로 확인되는 버전과 웹 서비스가 사용하는 버전이 다를 수 있으므로, 한 서버에 PHP가 여러 개 설치된 경우 각각 확인

※ 리눅스 배포판·제조사 제공 패키지는 보안 패치를 적용해도 버전 번호가 바뀌지 않을 수 있으므로, 패키지 변경 이력에서 CVE 반영 여부 확인

3. 구버전(PHP 8.1 이하)은 지원 버전으로 전환

o PHP 8.1 이하는 공식 업데이트가 제공되지 않으므로 지원 버전으로 전환

- PHP 8.2도 2026.12.31. 보안 지원이 종료될 예정이므로 8.3 이상 버전으로 전환 권장

o 전환에 시간이 걸리는 경우, 리눅스 배포판·장기지원(LTS) 업체가 제공하는 보안 패치 또는 PHP 보안팀이 공개한 7.4·8.0·8.1용 소스 패치를 임시로 적용하고 전환 계획 수립 [1]

o 적용할 패치가 없다면 수칙 4의 임시 조치를 적용하고, 그것도 어려우면 외부 접속 차단 또는 서비스 일시 중단 검토를 권고

4. 즉시 업데이트가 어려울 시 임시 조치 요망

o 웹 방화벽·웹 서버·프록시 등 PHP 앞단에서 요청 크기를 제한(요청 크기 정보가 없는 요청 포함)하고, 파일 업로드가 필요 없는 서비스는 파일 업로드(multipart) 요청을 차단

o 웹 방화벽을 이용 중이라면 최신 차단 규칙이 적용되었는지 확인

o PHP 공식 임시 설정을 php.ini, PHP-FPM pool 설정 또는 웹 서버 설정에 적용한 후 모든 PHP 프로세스 재시작 [1][2][3]

- session.upload_progress.enabled = 0 (파일 업로드 진행률 표시 기능 끄기)
- memory_limit = -1 (프로그램이 바꿀 수 없도록 관리자 설정으로 지정, 예: PHP-FPM pool의 php_admin_value)
- post_max_size 낮게 설정 (업로드가 필요 없으면 8M, 필요하면 32M 수준), upload_max_filesize는 post_max_size보다 작게 유지
- PHP 8.5 사용 시 fatal_error_backtraces = 0 추가

※ 임시 조치는 공격을 완전히 막지 못하므로, 업데이트 권고

o 임시 조치도 적용하기 어렵다면, 업데이트 전까지 외부 접속 차단 또는 서비스 일시 중단 검토를 권고

5. 업데이트 후 로그 점검

o 최소 10.20.(취약점 정보 유출일) 이후의 기록 전체를 점검하고, 가능하면 그 이전 기록까지 확인

o 주요 점검 항목

- PHP 페이지로 들어온 비정상적으로 큰 요청과 그 뒤에 반복된 서버 오류(HTTP 500)
- 원인을 알 수 없는 PHP 프로그램 재시작·비정상 종료(segfault)나 메모리 부족 오류
- 웹 서버가 명령 실행 프로그램(sh, bash 등)이나 파일 다운로드 도구를 실행한 흔적
- 웹 폴더, 업로드 폴더, 임시 폴더에 새로 생기거나 바뀐 PHP 파일(웹셸)
- 홈페이지나 결제 페이지에 몰래 추가된 외부 스크립트
- 웹 서버에서 알 수 없는 외부 주소로 새로 연결한 흔적

※ 기록상 이상이 없더라도 안전이 보장되지 않으므로, 업데이트와 인증정보 교체를 함께 진행

6. 중요 인증정보 교체

o 이번 취약점은 서버 메모리에 담긴 비밀번호, 접속 인증값(토큰), 외부 서비스 연동 키(API 키) 등을 유출시킬 수 있음 [3]

o 업데이트 전까지 인터넷에 노출되었던 서버는 DB 비밀번호, 외부 서비스 연동 키, 관리자 계정 비밀번호 교체 권장

- 침해 흔적이 발견된 서버는 반드시 교체

7. 침해사고 발생 시 아래 순서대로 대응

① 격리: 서버를 끄거나 재시작하지 말고, 네트워크에서 외부 접속만 차단

② 신고: [보호나라(https://boho.or.kr)] → [침해사고 신고] → [신고하기]를 통해 신고

③ 증거 확보: 서버 기록(로그), 실행 중인 프로그램 목록, 네트워크 연결 정보 보존

※ 서버를 재시작하면 메모리에 남은 공격 흔적이 사라지므로, 업데이트·재시작 전에 증거를 먼저 확보

④ 조치: 업데이트 및 재시작, 웹셸 제거, 인증정보 교체

8. 출처가 불분명한 PoC 실행 지양

o 인터넷에 유포되는 PoC 중에는 악성코드가 숨겨진 가짜가 많음

o 취약 여부는 PoC 실행 대신 버전 확인과 기록 점검으로 판단

o 분석이 꼭 필요한 경우 업무망과 분리된 환경에서만 수행

□ 참고사이트

[1] https://www.php.net/archive/2026.php#2026-10-21-5

[2] https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w

[3] https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp

[4] https://github.com/NCSC-NL/php2shell

[5] https://www.boho.or.kr/kr/bbs/view.do?searchCnd=&bbsId=B0000133&searchWrd=&menuNo=205020&pageIndex=1&categoryCode=&nttId=72227