[긴급/ 필독] 교내 웹사이트 및 정보시스템 보안 권고문

PHP 원격 코드 실행(RCE) 치명적 보안 취약점(php2shell) 발생에 따른 교내 웹사이트·정보시스템 긴급 점검 및 보안조치 안내

대상 취약점: CVE-2026-109618, CVE-2026-109619 (CVSS v4.0 9.2 Critical)
대상: 전 부서·학과·연구실·부속기관 홈페이지 및 웹 시스템 담당자

1. 취약점 개요 및 영향 범위

취약점 명칭 및 코드	PHP 비인증 원격 코드 실행(RCE) 취약점2건(일명'php2shell') •CVE-2026-109618(GHSA-w8hw-w9fx-j79w):OOM(메모리 부족) 손상을 통한 원격 코드 실행 •CVE-2026-109619(GHSA-6wmf-4rv5-p3rp):해제된 내부 전역 상태(Stale Global State) 재사용을 통한 원격 코드 실행
위험 등급(심각도)	**Critical (치명적) — CVSS v4.0 기준9.2점(즉각적인 패치 권고)**
취약점 상세 원리	• [CVE-2026-109618] 내부 요청 데이터가 부분적으로만 초기화된 상태에서 메모리 부족(OOM) 처리가 개입할 경우, 요청 정리(Cleanup) 단계에서 유효하지 않은 데이터를 정상 데이터로 오인하여 원격 코드 실행 발생 •[CVE-2026-109619]요청 소유 내부 상태가 백업 메모리 해제 후에도 잔존하여, 동일 워커(Worker)가 처리하는 후속 요청에서 정상 초기화 전에 해당 상태를 재사용하며 원격 코드 실행 발생
영향 받는 구동 환경	• 웹 요청을 처리하는 모든PHP 설치 환경: PHP-FPM, Apache(mod_php), php-cgi, FrankenPHP, LiteSpeed •특히Apache + mod_php 환경은 애플리케이션 코드가 실행되기도 전에 비인증 단일 요청만으로 공격이 트리거되는 실제 익스플로잇이 확인되어 위험도가 가장 높음
점검 대상 자산 범위	• 교내 각 부서·학과·연구실·사업단에서 자체 운영 또는 외부 웹호스팅/위탁 중인 웹사이트 및 웹 애플리케이션 •PHP가 내장(Embedded)된 상용 솔루션, 관리 인터페이스, 네트워크/보안 어플라이언스, Docker/컨테이너 이미지 전체
공식 해결버전	• PHP 8.5.12 / PHP 8.4.27 / PHP 8.3.36 / PHP 8.2.35 이상으로 즉시 업데이트 •PHP8.1이하(7.4, 8.0, 8.1): OS 벤더 배포 백포트(Backport) 패키지 또는PHP 보안팀 최소 소스 백포트 적용

2. 부서별 시스템 담당자 필수 조치 절차

(1단계) 유지보수 업체를 통한 시스템 현황 긴급 파악(즉시)

• 관리 중인 홈페이지 및 웹 시스템의 개발·유지보수 업체(또는 서버 관리자)에 본 공지사항을 즉시 전달합니다.
• 파악 필수 항목:
① PHP 사용 여부
② 현재 구동 중인 PHP 상세 버전
③ 웹 서버 연동 방식(mod_php, PHP-FPM 등)
④ 외부 인터넷 공개 여부
⑤ 패키지 설치 경로(OS 기본 저장소, Remi 저장소, 소스 컴파일, 컨테이너 여부)
•일반 웹사이트 외에 PHP가 번들링된 상용 웹 솔루션·장비 관리 페이지도 반드시 업체에 확인을 요청합니다

(2단계) 조치계획 수립 및 긴급 보안 패치(또는 임시 완화 조치) 적용

• [원칙: 정식 패치 즉시 적용] 구동 중인 브랜치별 최신 패치 버전(PHP 8.5.12 / 8.4.27 / 8.3.36 / 8.2.35) 또는OS 벤더 백포트 패키지로 즉시 업데이트합니다. (※ PHP 8.2는2026.12.31. 기술지원 종료(EOL) 예정이므로 상위 버전 전환 계획 병행 수립)

•[예외: 즉시 패치 불가 시 유지보수사를 통한 대책방안 수립] 서비스 호환성 검증 등으로 당일 업데이트가 불가능한 경우, 패치 완료 예정일(조치계획)을 수립하고 패치 전까지 유지보수사를 통한 임시대책을 반드시 확인합니다.

⚠보안 유의사항 및 침해 의심 징후 발견 시 행동 요령]

외부 접속이 가능한 시스템에서 보안 패치를 지연하거나 미승인 상태로 방치할 경우 침해사고의 직접적인 원인이 됩니다. 업체 점검 과정에서 비정상적인 대용량 요청, 반복적인 재시작(OOM), 웹셸(Webshell) 업로드 등 침해 의심 징후가 발견되면 임의로 포맷하거나 로그를 삭제하지 마시고(증거 보존) 즉시 IT운영팀(02-920-7383, ccenter@sungshin.ac.kr)으로 신고해 주시기 바랍니다.