[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

※ 외부 유지보수 개발업체 전달용 기술 가이드

본 기술 가이드는 성신여자대학교 웹사이트 및 정보시스템을 관리·위탁 운영하는 유지보수 업체 엔지니어를 위한 공식 조치 지침입니다. 2026년 10월 21일 발표된 PHP Security Advisory 및 CERT-EU 권고문(Advisory 2026-018) 기준에 따라 아래 조치를 즉시 이행해 주십시오.

1. 취약점 개요 및 영향 범위

구동중인 PHP버전	필수 업데이트 버전	패키지 저장소 및 기술지원(EOL) 유의사항
PHP 8.5.x 계열	**PHP 8.5.12 이상**	공식 소스, Windows 바이너리 또는 OS 벤더 최신 보안 패키지 즉시 적용
PHP 8.4.x 계열	**PHP 8.4.27 이상**	공식 소스, Windows 바이너리 또는 OS 벤더 최신 보안 패키지 즉시 적용
PHP 8.3.x 계열	**PHP 8.3.36 이상**	rpms.remirepo.net 사용 시 당일 즉시 업데이트 미제공 — OS 공식 배포판 패키지로 전환하거나 소스 빌드 즉시 적용 권고
PHP 8.2.x 계열 및 8.1 이하 구버전	**PHP 8.2.35 이상 (7.4/8.0/8.1은 백포트 적용)**	• PHP 8.2는 2026.12.31. 공식 지원 종료(EOL) 예정이므로 상위 버전 업그레이드 계획 수립 • PHP7.4/8.0/8.1은LTS 벤더 백포트 패키지 또는 PHP 보안팀 최소 소스 백포트 적용

2. 즉시 패치가 불가피하게 지연될 경우 임시 완화 조치

※ 완전한 해결책은 정식 버전 업데이트뿐이며, 패치 전까지 공격 노출 경로를 줄이기 위해 아래 설정을 요청 파싱 전 단계(php.ini, FPM pool, Apache 설정 내 php_admin_value)에 적용하고 반드시 모든 워커(Worker)를 재시작하십시오. (ini_set() 또는 .user.ini 의존 금지)

대상 취약점 코드	필수 임시 완화 설정 및 서버 구성 지침(재시작 필수)
CVE-2026-109618 (RCEviaOOMCorruption)	1) 메모리 제한 해제: FPM pool 또는Apache 설정에서 애플리케이션이 덮어쓸 수 없도록 php_admin_value[memory_limit] = -1 설정(하위 풀·디렉터리·앱 코드에서 유한 값으로 재설정하지 않는지 전수 확인) 2)요청 본문 크기 축소: 파일 업로드 불필요 시post_max_size = 8M, 업로드 필요 시 post_max_size = 32M 이하로 설정하고upload_max_filesize를post_max_size 미만으로 유지. 웹 서버/프록시/WAF 앞단에서 디코딩된 요청 크기, 입력 필드 수, 멀티파트 수, 헤더 수, 중첩 깊이 제한 강제(Content-Length 미포함 요청 포함) 3)가용성 경계(Availability Boundary) 설정: 컨테이너 또는cgroup 메모리 제한을 사용하여 문제 발생 워커만 개별 종료(Kill)되도록 구성(※ 주의: RLIMIT_AS 또는RLIMIT_DATA는 취약한 메모리 할당 실패를 직접 유발하므로 절대 대체 사용 금지)
CVE-2026-109619 (RCEviaStaleGlobalState)	1) 세션 업로드 진행상태 비활성화: php.ini, FPM pool 또는 서버 설정에서 session.upload_progress.enabled = 0 적용 후 모든 워커 프로세스 재시작 2)치명적 오류 백트레이스 비활성화(PHP 8.5): PHP 8.5 환경에서는fatal_error_backtraces = 0 설정 후 모든 워커 재시작 3)초기화 전 진단 출력 설정 제거: 요청 초기화 이전에 진단(Diagnostics)을 발생시키는 잘못되거나 폐기된(Deprecated) 요청별 설정 제거(error_reporting, display_errors, @ 연산자로 화면 출력을 숨기는 것은 방어 효과 없음) 4)공격자 유발 오류 수정: 콜백, 업로드/임포트 처리 및 정리(Cleanup) 과정에서 외부 요청으로 도달 가능한Fatal Error 및 실행 타임아웃 경로 점검·수정