EG엣지넷

TECHNICAL WHITEPAPER · 2026.10

PHP2Shell 공격, UWSS WEBCastle로 차단합니다

CVE-2026-109618 · CVE-2026-109619 대응 기술 백서

공격 원리 · 탐지·차단 방식 · 실장비 검증 결과 · 도입 효과

80/80	9/9	0건	100%
공격 패턴 차단(HTTP 403)	정상 요청 통과 · 오탐 0건	5xx 서버 오류	기대 결과 일치 (89/89)

㈜엣지넷 · UWSS(Unified Web Security Service) · https://www.mireene.com

요약 (Executive Summary)

2026년 10월 공개된 **PHP2Shell**(CVE-2026-109618, CVE-2026-109619)은 PHP 애플리케이션 코드가 실행되기 전, **PHP 엔진이 HTTP 요청 본문을 해석(파싱)하는 단계**에서 발생하는 원격 코드 실행(RCE) 취약점입니다. 웹사이트 소스가 안전하더라도 취약한 PHP 런타임 위에서 동작한다면 공격 대상이 될 수 있습니다.

엣지넷은 UWSS의 서버 밀착형 웹방화벽 **WEBCastle**에 PHP2Shell 전용 탐지 정책(정책 그룹 4202)을 배포하고, 실제 공격 패 턴을 무해하게 재현한 89건의 요청으로 차단 효과를 검증했습니다.

89	80	9	0
검증 요청	공격 패턴 → 전부 403 차단	정상 대조군 → 전부 통과	5xx 오류

핵심 메시지

- PHP 패치 적용 전이라도 WEBCastle 정책 적용만으로 PHP2Shell 공격 요청을 웹서버·PHP 도달 전에 차단
- 공격 원리(긴 필드명·비정상 멀티파트·세션 업로드 진행률 악용)에 맞춘 구조 기반 탐지로 정상 업로드·폼 전송은 통과
- 모든 탐지·차단 이벤트를 UWSS 콘솔에서 정책 ID·요청 상세와 함께 즉시 확인

본 문서는 공격 원리를 개념 수준으로만 설명하며, 실행 가능한 공격 코드(PoC/Exploit)를 포함하지 않습니다. 검증에 사용된 요청은 모두 원격 코드 실행을 일으키지 않는 무해한 탐지 패턴입니다. WAF는 위험을 줄이는 보완 통제이며, 근본 조치는 PHP 보안 업데이트 적용입니다.

1. PHP2Shell 취약점 개요

PHP2Shell은 두 개의 취약점으로 구성됩니다. 두 취약점 모두 SQL 인젝션·XSS처럼 "악성 문자열"을 담는 공격이 아니라, **요청의 구조와 크기** 및 **PHP 내부 상태**를 악용한다는 점에서 기존 웹 공격과 성격이 다릅니다.

CVE-2026-109618 — 긴 필드명·요청 본문 처리 과정의 메모리 손상

- 공격자는 폼 필드명 또는 멀티파트 파트 헤더의 **name 값을 비정상적으로 길게(수천 바이트 이상)** 구성한 요청을 보냅니다.
- PHP가 이를 파싱하는 과정에서 메모리 한도에 도달하면, 정리(cleanup) 과정이 불완전하게 수행되어 메모리 손상이 발생하고 원격 코드 실행으로 이어질 수 있습니다.
- URL 인코딩 본문, 멀티파트 업로드, 형식이 깨진 본문 등 여러 전달 경로가 존재합니다.

CVE-2026-109619 — 세션·업로드 진행률·직렬화 경로 악용

- 멀티파트 업로드에 **PHPSESSID를 폼 필드로 주입**하고 PHP의 **세션 업로드 진행률(session.upload_progress)** 기능을 함께 이용합니다.
- 업로드 **파일명**에 PHP 코드 여는 태그나 **직렬화 객체 구문**을 넣어, 세션 저장소에 공격자 데이터가 기록되도록 유도합니다.
- 앞선 요청이 남긴 PHP 워커 상태가 다음 요청에 재사용되는 구조여서, 요청 하나만 보고 판단하기 어렵습니다.

구분	CVE-2026-109618	CVE-2026-109619
공격 지점	필드명 길이 · 본문 파싱	세션 ID · 업로드 진행률 · 파일명
특징	악성 문자열 없이 크기·구조만으로 유발	여러 요청에 걸친 상태 오염
영향	원격 코드 실행 → 웹쉘 설치 · 서버 장악 · 데이터 유출	

영향 범위. 지원 종료(EOL) 버전을 포함해 다양한 PHP 버전이 운영 중인 국내 환경 특성상, 즉시 패치가 어려운 서버가 많습니다.

2. 기존 대응 방식의 한계

기존 방식	한계
PHP 패치 대기	호환성 시험·재시작 일정 때문에 적용까지 수일~수주 소요. EOL 버전은 공식 패치가 없어 재빌드 필요. 그 사이 서비스는 무방비 상태
임시 설정 변경	memory_limit 조정 등 우회 조치는 서버 전체 메모리 고갈(DoS) 등 부작용 위험
일반 WAF 시그니처	공격에 고정된 "악성 문자열"이 없어 문자열 매칭만으로는 미탐 또는 정상 업로드 과탐 발생. 과탐 우려로 정책을 탐지 전용으로만 두는 경우가 많음
본문 검사 크기 제한	성능 때문에 요청 본문 앞부분만 검사하는 구성에서는 검사 범위를 벗어난 데이터를 인지하지 못할 수 있음
경계형(네트워크) 단독 방어	한 번 우회되면 서버 내부의 웹쉘 생성·실행을 확인할 수단이 없음

주요 글로벌 WAF 벤더도 관련 탐지 규칙을 배포하고 있습니다. 중요한 것은 "정책이 존재하는가"가 아니라 **고객 환경에서 차단 모드로 실제 동작하는지, 그리고 그 증적을 제시할 수 있는지**입니다.

3. UWSS WEBCastle의 대응 방식

① 구조 기반 탐지
필드명 길이(1000자/바이트 경계), 멀티파트 파트 헤더, 본문 파싱 실패, 멀티파트 엄격 검증 등 **요청 구조**를 직접 검사합니다. 문자열이 없어도 공격 조건을 판별합니다.

② 공격 체인 결합 탐지
멀티파트 업로드 + 업로드 진행률 + PHPSESSID 주입처럼 **공격 단계의 조합**을 하나의 정책으로 판별하고, 파일명 내 PHP 태그·직렬화 구문을 차단합니다.

③ 서버 밀착형 에이전트
WEBCastle은 고객 웹서버에서 동작하여 기존 네트워크 구성 변경 없이 적용되며, 웹서버·PHP 처리 전 단계에서 요청을 차단합니다.

④ 중앙 관리·가시성
UWSS 콘솔에서 정책을 일괄 배포하고, 탐지·차단 이벤트를 정책 ID·요청 헤더·매칭 근거와 함께 확인합니다.

탐지 정책 구성 (정책 그룹 4202)

CVE-2026-109618 대응 5종(긴 필드명 3개 경로 + 파싱 실패 + 멀티파트 엄격 검증), CVE-2026-109619 대응 4종(PHPSESSID 주입, 파일명 PHP 태그, 파일명 직렬화 구문, 3단 결합 체인)으로 구성됩니다. 정책별 상세는 부록 A에 수록했습니다.

4. 실제 적용 화면: 공격 발생부터 확인까지

① PHP2Shell 공격 발생 | ② WEBCastle 탐지·차단 | ③ UWSS 콘솔 탐지 로그 | ④ 적용 정책·상세 정보

① 공격 발생 → ② 차단. 공격자가 긴 필드명, 비정상 멀티파트, 파일명 PHP 태그 등 PHP2Shell 조건을 갖춘 요청을 보내면, WEBCastle이 웹서버·PHP 처리 전에 이를 판별하여 **HTTP 403**으로 차단합니다. 정상 요청은 그대로 서비스됩니다.

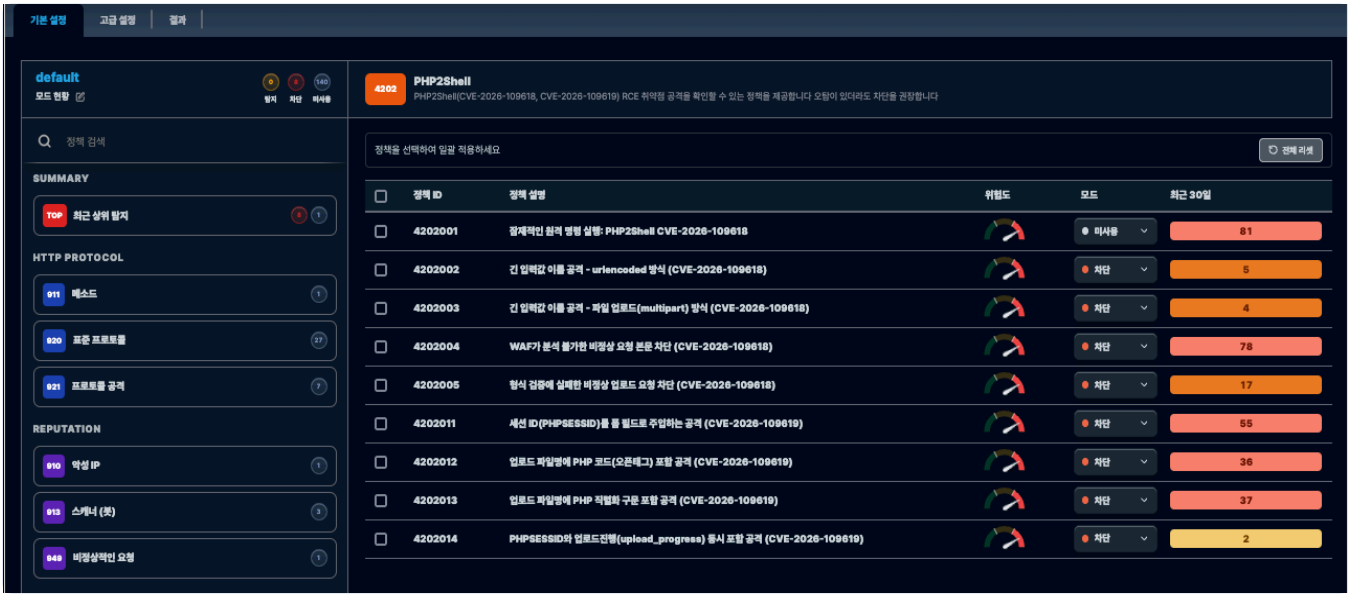


그림 1. UWSS 콘솔 — PHP2Shell 정책 그룹(4202) 구성 및 최근 30일 탐지 현황

③ 탐지 로그 확인. 차단된 요청은 실시간으로 UWSS 콘솔 탐지 로그에 기록되며, 어떤 정책(공격 유형)에 의해 차단되었는지 한눈에 확인할 수 있습니다.

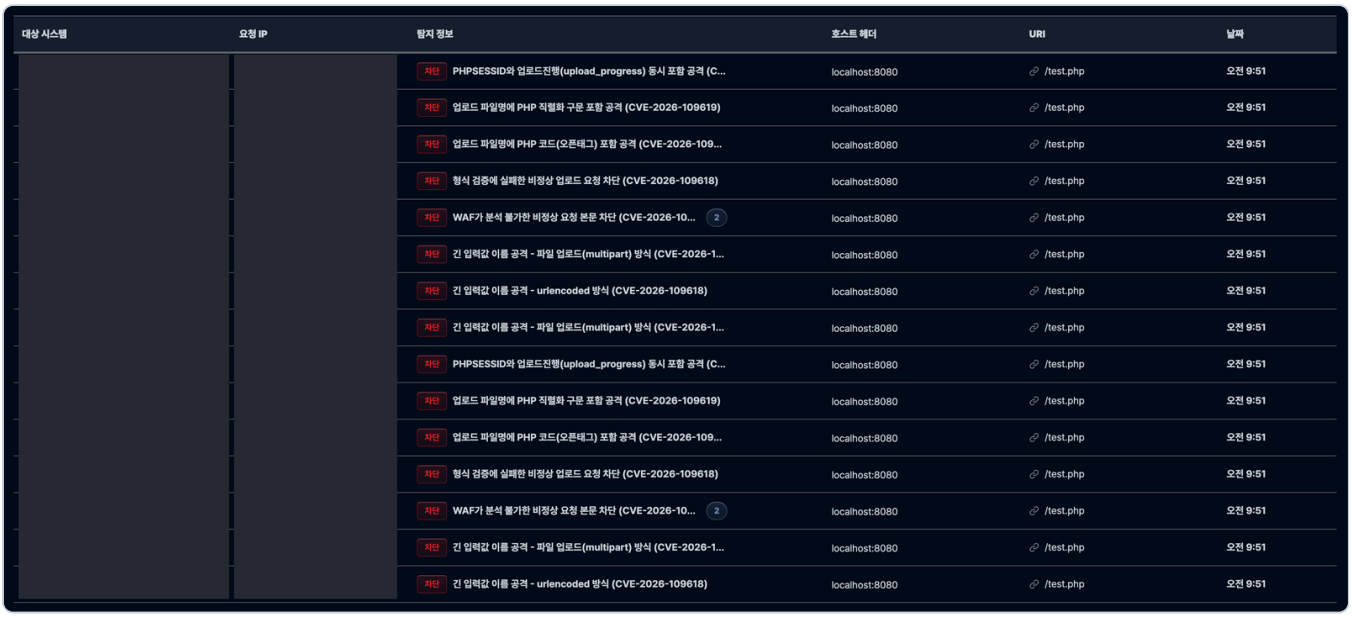


그림 2. UWSS 콘솔 탐지 로그 — PHP2Shell 유형별 '차단' 이벤트 (대상 시스템·요청 IP는 마스킹)

④ 적용 정책 및 상세 정보. 개별 로그를 열면 탐지 정책 ID, 매칭 근거(검사 변수와 조건), 요청 메서드·헤더·크기 등 사고 분석에 필요한 정보를 제공합니다. 아래 예시는 업로드 파일명에 PHP 여는 태그가 포함된 요청(CVE-2026-109619 경로)이 정책 4202012로 차단된 기록입니다.



그림 3. WEBCastle 상세 로그 — 탐지 정책 ID 4202012, 매칭 근거, HTTP 요청 정보 (호스트 식별자·IP 마스킹)

5. 검증 결과

검증 방법

- 대상: PHP2Shell 정책 그룹(4202)이 적용된 UWSS WEBCastle 실장비 환경
- 요청: 공격 원리별 무해한 탐지 패턴 80건 + 정상 대조군 9건(경계값 직전 길이, 정상 업로드·폼 전송 등), 총 89건
- 판정: 공격 패턴은 HTTP 403(차단), 대조군은 HTTP 200(통과)일 때 기대 일치
- 범위: PHP2Shell 공격 체인에서 확인된 경로를 대상으로 하며, 공격 체인과 무관한 일반 멀티파트 형식 오류 변형은 제외

45/45	35/35	9/9	89/89
CVE-2026-109618 공격 차단	CVE-2026-109619 공격 차단	정상 요청 통과	기대 일치 100%

구분	공격 패턴	403 차단	정상 대조군	200 통과	5xx
CVE-2026-109618	45	45	4	4	0
CVE-2026-109619	35	35	5	5	0
합계	**80**	**80**	**9**	**9**	**0**

해석. 공격 원리별 대표 변형(길이 경계값, 인코딩·전달 경로 변형, 체인 조합)을 모두 차단하면서, 경계 직전 길이의 정상 필드명이나 일반 업로드는 통과시켰습니다. 서버 오류(5xx)가 한 건도 없어, 차단이 서비스 안정성에 영향을 주지 않음을 확인했습니다.

6. 차별성 및 고객 보안 효과

비교 항목	일반 대응	UWSS WEBCastle
대응 시점	PHP 패치 적용까지 노출	정책 배포 즉시 차단 — 패치 전 가상 패치(Virtual Patch) 역할
탐지 방식	문자열 시그니처 중심	요청 구조·공격 체인 기반 판별
오탐 관리	과탐 우려로 탐지 전용 운영	정상 대조군 9/9 통과 검증 후 차단 모드 운영
도입 부담	장비 도입·네트워크 변경	서버 에이전트 + 클라우드 중앙관리, 기존 WAF와 병행 가능
증적	정책 제공 여부만 안내	실장비 89건 검증 결과 + 콘솔 로그로 차단 사실 입증

고객이 얻는 효과

보안 공백 해소
패치 시험·적용 기간 동안 PHP2Shell 공격을 즉시 차단하여 RCE·웹쉘 설치 위험을 낮춥니다.

서비스 연속성
정상 업로드·폼 전송은 통과, 서버 오류 0건 — 운영 중단 없이 적용합니다.

가시성과 설명 책임
정책 ID·매칭 근거가 담긴 로그로 차단 사실을 경영진·감사 대응에 제시할 수 있습니다.

기존 투자 보호
기존 WAF를 유지한 채 서버 단 보호를 추가하는 병행 도입이 가능합니다.

권장 도입 절차

무료 자가진단 → 위험 확인 (PHP 버전·구성) → WEBCastle 정책 적용 (차단 검증) → PHP 보안 업데이트 (근본 조치)

무료 자가진단은 정상 요청만 사용하여 노출 가능성을 안내하는 도구로, 실제 취약 여부를 확정하지 않습니다.

부록 A. PHP2Shell 탐지 정책 목록

정책 ID	CVE	탐지 내용	공격 차단	대조군 통과
4202001	2026-109618	파싱된 폼 필드명 길이 ≥ 1000자	9/9	1/1
4202002	2026-109618	URL 인코딩 본문 원시 필드명 ≥ 1000바이트	9/9	1/1
4202003	2026-109618	멀티파트 파트 헤더 name= ≥ 1000자	9/9	1/1
4202004	2026-109618	요청 본문 파싱 실패	9/9	1/1
4202005	2026-109618	멀티파트 엄격 검증 실패	9/9	0/–
4202011	2026-109619	멀티파트 폼 필드로 PHPSESSID 주입	7/7	3/3
4202012	2026-109619	업로드 파일명에 PHP 여는 태그	10/10	0/–
4202013	2026-109619	업로드 파일명에 직렬화 객체 구문	10/10	0/–
4202014	2026-109619	멀티파트 + 업로드 진행률 + PHPSESSID 결합	8/8	2/2

정책 ID는 UWSS 콘솔 탐지 로그의 '탐지 정책 ID'와 동일합니다. 경계값 1000은 정상 서비스에서 사용되지 않는 길이를 기준으로 설정되었습니다.

부록 B. 용어

용어	설명
멀티파트(multipart/form-data)	파일 업로드 등에 쓰이는 HTTP 본문 형식
session.upload_progress	업로드 진행 상황을 세션에 기록하는 PHP 기능
직렬화 객체	PHP 객체를 문자열로 저장한 형태. 역직렬화 시 악용될 수 있음
가상 패치	코드·런타임 수정 없이 보안 정책으로 취약점 악용을 차단하는 방식

문의 ㈜엣지넷 · https://www.mireene.com

본 문서의 내용은 작성 시점 기준이며, 제품 기능과 정책은 업데이트될 수 있습니다. UWSS, WEBCastle은 ㈜엣지넷의 제품명입니다.