최신 웹 공격 관련 연구 결과 소개 CVE-2025-22777

> [19반] 정민석_7000

내용 요약

CVE-2025-22777 취약점은 2025년 01월13일에 발표된 WordPress의 GiveWP라는 기부 플러그인에서 발생한 취약점입니다. 해당 취약점은 3.19.3 이하의 버전에서 유효합니다. 해당 취약점을 통하여 악의적인 행위자는 악성 페이로드를 심고, 이는 추후 역직렬화되어 wp-config.php 등을 포함한 파일 삭제를 시도할 수 있습니다. 이로 인하여, RCE/사이트 장악 등이 가능합니다.

취약점의 근본 원인 및 공격방법

이 취약점은 문자열에 대한 약한 정규 표현식 검사로 인하여 발생합니다. 따라서 공격 방법 또한 정규 표현식 검사를 우회하는 방향으로 진행될 수 있습니다.

Patchstack의 보안 연구원 Ananda Dhakal은 "*_문자열의 약한 정규 표현식 검사로 인해 직렬화된 전체 검사가 우회될 수 있었습니다. 공격자는 정규 표현식 검사를 무효화하고 결국 역직렬화될 DB에 악성 메타데이터를 저장할 수 있는 난해한 텍스트를 직렬화된 페이로드 사이에 입력할 수 있습니다* ." 라고 설명합니다. Patchstack Alliance 회원이자 Zalopay Security의 Edisc는 %25F0%259F%2598%25BC와 같은 특수 문자 시퀀스를 주입하여 취약한 정규 표현식 검증을 우회함으로써 이 취약점을 악용할 수 있었습니다.[2]

공격의 파급도

WordPress의 GiveWP라는 플러그인은 활성 설치가 100,000건이 넘습니다. GiveWP 플러그인은 WordPress의 기부 플러그인 중 가장 많이 다운로드된 플러그인 중 하나입니다. 이처럼 많은 사용자에게 영향을 미칠 수 있는 취약점이 공개되었고, CVSS 점수가 9.8을 기록하였습니다.

방어 방법

먼저 사용자는 취약점이 패치된 3.19.4 이상의 버전으로 업그레이드를 진행해야할 것입니다. 더하여 GiveWP 플러그인의 개발자는 아래의(전체 코드는 [3]의 링크 참조) 코드를 추가하는 등, 약한 정규 표현식을 엄격하게 검사하는 방향으로 패치를 진행하였습니다.

```
public static function recursiveUrlDecode(string $data): string
{
  $decoded = urldecode($data);
```

```
    return $decoded === $data ? $data : self::recursiveUrlDecode($decoded);
}
```

취약점 관련 자료를 수집한 방법

먼저 구글에 CVE-2025-22777의 키워드로 검색한 결과 [1], [2], [4]의 링크를 찾아볼 수 있었습니다. 더하여 Github에서 GiveWP에 대한 소스코드를 검색하였고, 해당 레포지터리에서 [5]와 같이 3.19.3과 3.19.4 버전의 소스코드를 비교하여 패치 변경점을 확인하였습니다. 그 결과 [3]과 같이 정규 표현식에 대한 검사를 강화한 패치 내역을 확인 할 수 있었습니다.

[참고 문헌]

- [1] https://nvd.nist.gov/vuln/detail/CVE-2025-22777
- [2] https://securityonline.info/cve-2025-22777-cvss-9-8-critical-security-alert-for-givewp-plugin-with-100000-active-installations/
- [3] https://github.com/impress-org/givewp/commit/d2bdcdee8c35661ec6eceef923f2ecf7944f01f4
- [4] https://patchstack.com/database/wordpress/plugin/give/vulnerability/wordpress-givewp-plugin-3-19-3-php-object-injection-vulnerability?_s_id=cve
- [5] https://github.com/impress-org/givewp/compare/release/3.19.3...release/3.19.4