Zoho Lead Magnet Version 1.7.2.4에서 양식 값을 변경하거나 생성된 양식을 삭제할 때 마다 Stored XSS 페이로드가 실행되는 취약점

취약한 버전

Zoho CRM Lead Magnet 버전 1.7.2.4

개념

Zoho란?

Microsoft Office나 Google Workspace와 같은 클라우드 기반 소프트웨어 제품군

CRM?

고객관계관리로 연락처, 계정, 거래 등 판매 프로세스와 고객 커뮤니케이션을 관리하는 플러그인

취약점 공격 방법

동작 과정

1. 애플리케이션에 로그인을 한다.
2. 취약한 버전인 Zoho CRM 리드 매그넷 플러그인을 설치한다. (1.7.2.4 버전)
3. 클라이언트 ID와 비밀 키를 구성한다.
   -> Zoho CRM 플러그인 양식 값을 입력한다.
4. 페이로드 `<img src=x onerror=alet(document.cookie)>`를 16진수 HTML 인코더로 인코딩한다.
   -> src=x 주소의 img를 불러온다. 이때 에러가 발생하면 cookie값을 띄운다.
5. '양식 이름'필드에 인코딩된 페이로드를 입력하여 양식을 업데이트 한 후 이전 페이지 버튼을 눌러 이전 페이지로 돌아간다.
6. 생성된 양식의 '회사'나 '성'등의 양식 값을 변경한다.
   -> XSS 페이로드는 사용자가 양식을 수정하거나 삭제하려고 할 때 실행된다.

영향

1. 쿠키 도용
2. 최종 사용자 파일 공개
3. 트로이 목마 프로그램 설치
4. 사용자를 다른 페이지 또는 사이트로 리다이렉션

취약점 방어

1. 인코딩 라이브러리를 사용하여 신뢰할 수 없는 입력을 브라우저로 다시 전송하기 전에 상황에 맞는 인코딩을 수행
2. 브라우저에 반영되고 데이터베이스에 저장되는 모든 변수에 대한 특수 문자에 대한 입력 유효성 검사를 구현
3. 클라이언트 측 유효성 검사를 구현

---

https://www.securin.io/zerodays/cve-2021-33849-stored-cross-site-scripting-in-wordpress-plugin-zoho-crm-lead-magnet-version-1-7-2-4/