Zeroboard 다중 취약점들

Systems Affected

ZeroBoard 4.1pl7 이하의 버전들

I.Description

o **IP session bypass XSS vulnerability**

- 발전된 XSS 공격으로서 zeroboard에서 XSS 공격으로 Session ID를 도용하는 것에 대한 방비책으로 IP를 검사하는 것을 우회 할 수 있다. 공격자는 쪽지의 제목 등에 iframe 태그를 삽입하여 관리자가 자신도 모르는 사이에 웹 상의 임의의 파일을 실행하도록 할 수 있다.

o **SQL Injection vulnerability**

- 관리자나 일반 사용쪽을a대대다태등대쪽등m을일우있지을반우Q드실격지제다태등대자대드게의대쪽을자우있

o 벤더의 최신 패치 적용

http://www.nzeo.com/ 에서 현재 가장 최신 버전인 **4.1 pl8** 을 다운로드 받아서 설치한다.

4.1 pl7 버전을 사용하고 있다면 다음의 파일들만 찾아서 교체한다.

image_box.php
member_join_ok.php
member_modify_ok.php
login_check.php
lib.php
member_memo.php
member_memo2.php
member_modify_ok.php
license.txt

참고 사이트

http://www.inetcop.org/upfiles/33INCSA.2006-0x82-029-zeroboard.pdf

http://www.nzeo.com/bbs/zboard.php?id=cgi_download2&page=1&sn1=&divpage=1&sn=off&ss=on&sc=off&select_arrange=headnum&desc=asc&no=53