



Site Search



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)

List Archive Search



[SYSS-2021-042] TJWS - Reflected Cross-Site Scripting (CVE-2021-37573)

From: Maurizio Ruchay <maurizio.ruchay () syss de>

Date: Wed, 11 Aug 2021 08:46:11 +0200

Advisory ID: SYSS-2021-042
Product: Tiny Java Web Server and Servlet Container (TJWS)
Manufacturer: D. Rogatkin
Affected Versions: <= 1.115
Tested Versions: 1.107, 1.114
Vulnerability Type: Cross-Site Scripting (CWE-79)
Risk Level: Medium
Solution Status: Fixed
Manufacturer Notification: 2021-07-21
Solution Date: 2021-07-23
Public Disclosure: 2021-08-03
CVE Reference: CVE-2021-37573
Author of Advisory: Maurizio Ruchay, SySS GmbH

Overview:

Tiny Java Web Server and Servlet Container (TJWS) is a lightweight web server written in Java.

The manufacturer describes the product as follows (see [1]):
"The Miniature Java Web Server is built as a servlet container with HTTPD servlet providing standard Web server functionality."

Due to improper input validation, the application is vulnerable to a reflected cross-site scripting attack.

Vulnerability Details:

It is possible to inject malicious JavaScript code into the server's error page "404 Page Not Found".

The given input is not properly validated and therefore reflected back and executed in a victim's browser.

Proof of Concept (PoC):

The following GET request shows how JavaScript code can be placed on the page:

===

HTTP request:
GET /te%3Cimg%20src=x%20onerror=alert(42)%3Est HTTP/1.1
[...]
Connection: close

HTTP response:
HTTP/1.1 404 test not found
server: D. Rogatkin's TJWS (+Android, JSR340, JSR356) <https://github.com/drogatkin/TJWS2.git/Version> 1.114
[...]
content-length: 338
connection: close

<HTML><HEAD><TITLE>404 test not found</TITLE></HEAD><BODY BGCOLOR="#D1E9FE">
[...]
<H2>404 test not found</H2>
[...]
===

If a browser renders the response, the JavaScript code is executed showing the message "42".

Solution:

The issue has been addressed in the release version 1.116.[2]
Therefore, all instances of TJWS should be updated to this version.

Disclosure Timeline:

2021-07-02: Vulnerability discovered
2021-07-21: Vulnerability reported to manufacturer
2021-07-23: Patch released by manufacturer
2021-08-03: Public disclosure of vulnerability

References:

- [1] Product website for Tiny Java Web Server and Servlet Container (TJWS): <http://tjws.sourceforge.net/>
- [2] Patch release on Github: <https://github.com/drogatkin/TJWS2/releases/tag/v1.116>
- [3] SySS Responsible Disclosure Policy <https://www.syss.de/en/responsible-disclosure-policy>

Credits:

This security vulnerability was found by Maurizio Ruchay of SySS GmbH.

E-Mail: maurizio.ruchay () syss de
Public Key: https://www.syss.de/fileadmin/dokumente/PGPKeys/Maurizio_Ruchay.asc
Key ID: 0xC7D20E267F0FA978
Key Fingerprint: D506 AB5A FE3E 09AE FFBE DEB2 C7D2 0E26 7F0F A978

Disclaimer:

The information provided in this security advisory is provided "as is" and without warranty of any kind. Details of this security advisory may

be updated in order to provide as accurate information as possible. The latest version of this security advisory is available on the SySS Web site.

Copyright:

Creative Commons - Attribution (by) - Version 3.0
URL: <https://creativecommons.org/licenses/by/3.0/deed.en>





Attachment: [OpenPGP signature](#)
Description: OpenPGP digital signature

Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <http://seclists.org/fulldisclosure/>

[◀ By Date ▶](#) [◀ By Thread ▶](#)

Current thread:

[SYSS-2021-042] TJWS - Reflected Cross-Site Scripting (CVE-2021-37573) *Maurizio Ruchay (Aug 13)*

Nmap Security Scanner	Npcap packet capture	Security Lists	Security Tools	About	 
Ref Guide	User's Guide	Nmap Announce	Vuln scanners	About/Contact	
Install Guide	API docs	Nmap Dev	Password audit	Privacy	 
Docs	Download	Full Disclosure	Web scanners	Advertising	
Download	Npcap OEM	Open Source Security	Wireless	Nmap Public Source License	
Nmap OEM		BreachExchange	Exploitation		