<UWE-484-01>: <Description/Title>

Authors:

The Basics

Disclosure Date: 11/24/2021
Product: tinyserv
Reporter(s): CSE 484 Staff

The Code

Exploit sample: see sploit1.c
Did you have access to the exploit sample when doing the analysis? yes

The Vulnerability

Bug class (1p):
Vulnerability details (3p):
Thoughts on how this vuln might have been found (fuzzing, code auditing, variant analysis, etc.) (1p):

The Exploit

(The terms exploit primitive, exploit strategy, exploit technique, and exploit flow are defined here.)
Exploit primitive (1p):
Exploit strategy (or strategies) (2p):

The Next Steps

Proposed patch plan (2p):

What are potential detection methods for similar 0-day vulnerabilities? (bonus 1p):

<UWE-484-02>: <Description/Title>

Authors:

The Basics

Disclosure Date: 11/24/2021
Product: tinyserv
Reporter(s): CSE 484 Staff

The Code

Exploit sample: see sploit2.c
Did you have access to the exploit sample when doing the analysis? yes

The Vulnerability

Bug class (1p):
Vulnerability details (3p):
Thoughts on how this vuln might have been found (fuzzing, code auditing, variant analysis, etc.) (1p):

The Exploit

(The terms exploit primitive, exploit strategy, exploit technique, and exploit flow are defined here.)
Exploit primitive (1p):
Exploit strategy (or strategies) (2p):

The Next Steps

Proposed patch plan (2p):

What are potential detection methods for similar 0-day vulnerabilities? (bonus 1p):