Talos Vulnerability Report

TALOS-2020-1069

Siemens LOGO! Web Server Code Execution Vulnerability

JULY 15, 2020

CVE NUMBER

CVE-2020-7593

Summary

An exploitable code execution vulnerability exists in the Web Server functionality of Siemens LOGO! 1.82.02, 12/24RCE Version 0BA and 230RCE Version 0BA. A specially crafted HTTP request can cause memory corruption resulting in a code execution. An attacker can send an unauthenticated packet to trigger this vulnerability.

Tested Versions

Siemens LOGO! 1.82.02
Siemens LOGO! 12/24RCE Version 0BA
Siemens LOGO! 230RCE Version 0BA

Product URLs

https://new.siemens.com/global/en/products/automation/systems/industrial/plc/logo.html

CVSSv3 Score

10.0 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-120 - Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’)

Details

Siemens LOGO! is an intelligent logic module (PLC) meant for automation projects such as industrial control systems, office/commercial and home settings. It is deployed worldwide and can be control remotely.

The HTTP Server for the LOGO! system doesn’t properly check the length of a URI directory before copying the URI to the stack, resulting in a stack overflow. Our research and testing indicates that the cause of this crash resides within the u_bm3.bin firmware image at address 0x9be8e:

0009BE84 A5 EB 07 0A SUB.W R10, R5, R7 # r10 = length of URI between opening/closing slashes 0009BE88 52 46 MOV R2, R10 # len - our user-controlled length 0009BE8A 39 46 MOV R1, R7 # src - the URI requested 0009BE8C 05 A8 ADD R0, SP, #0x14. # destination stack address 0009BE8E D7 F7 0F FA BL call_memcpy # overflow the stack 0009BE92 05 A8 ADD R0, SP, #0x78+requested_dir_without_slashes ; s1 0009BE94 00 21 MOVS R1, #0 0009BE96 0A F8 00 10 STRB.W R1, [R10,R0] ; NULL terminate the copied URI dir on the stack

Exploit Proof of Concept

curl http://<LOGO!IP>/`python -c 'print("A" 100)'`/

Timeline

2020-05-07 - Vendor Disclosure

2020-07-14 - Vendor Patched
2020-07-15 - Public Release

CREDIT

Discovered by Alexander Perez-Palma and Dave McDaniel of Cisco Talos and Emanuel Almeida of Cisco Systems, Inc.
