Talos Vulnerability Report

TALOS-2020-1003

3S-Smart Software Solutions GmbH CODESYS Runtime PLC_Task Code Execution Vulnerability

MAY 6, 2020

CVE NUMBER

CVE-2020-6081

Summary

An exploitable code execution vulnerability exists in the PLC_Task functionality of 3S-Smart Software Solutions GmbH CODESYS Runtime 3.5.14.30. A specially crafted network request can cause remote code execution. An attacker can send a malicious packet to trigger this vulnerability.

Tested Versions

3S-Smart Software Solutions GmbH CODESYS Runtime 3.5.14.30

Product URLs

https://www.codesys.com/

CVSSv3 Score

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

CWE

CWE-345 - Insufficient Verification of Data Authenticity

Details

The CODESYS Control SoftPLC runtime system converts any embedded or PC-based device into an IEC 61131-3-compliant industrial controller. Furthermore, this runtime system includes important add-on functionality so that your controller can communicate with other components in the automation environment.

Application code for CODESYS is compiled down to native machine code when sent from the programming software. This machine code is only subjected to a CRC32 check before being executed in the context of the codesys3 binary in a separate thread. By building an .app file with architecture appropriate shellcode an attacker can get remote code execution with the ability to upload projects. This upload can occur over SSH or the Codesys port 11740 using the proprietary protocol. In order to pass the CRC check, a .crc file has to be created with the CRC32 of the entire .app file.

This vulnerability exists due to the lack of enforcing cryptographic verification on the uploaded binary blob. Since authentication can be disabled for the port 11740 used for uploading PLC applications to the device, a cryptographic signature is required in order to verify that the binary comes from a trusted source. Without cryptographic verification, in the event that a device was configured to block all direct access to the device other then required application logic following IEC 61131 standards, arbitrary code could be executed directly on the device with the privileges associated with the Codesys runtime.

Crash Information

```
──────────────────────────────────────────────────────────────── code:arm:ARM ────
0xb4387d6c                  push   {r11,  lr}
0xb4387d70                  mov    r11,  sp
0xb4387d74                  sub    sp,  sp,  #0
 → 0xb4387d78                  b      0xb4387d78
0xb4387d7c                  andvs  r0,  r0,  r0
0xb4387d80                  mov    lr,  pc
0xb4387d84                  mov    pc,  r4
0xb4387d88                  ldrb   r4,  [sp,  #8]
0xb4387d8c                  add    sp,  sp,  #16

───────────────────────────────────────────────────────────────────── threads ────
* 26   Thread 21998.22060 "PLC_Task" 0xb4387d78 in ?? ()
```

Timeline

2020-02-05 - Vendor Disclosure

2020-05-06 - Public Release

CREDIT

Discovered by Carl Hurd of Cisco Talos.