Security Advisory
Vulnerabilities in CODESYS V2 runtime systems

1 Advisory Information

Advisory ID: BOSCH-SA-670099
CVE Numbers and CVSS v3.1 Scores:

- CVE-2021-30186
  - Base Score: 7.5 (High)
- CVE-2021-30188
  - Base Score: 9.8 (Critical)
- CVE-2021-30189
  - Base Score: 9.8 (Critical)
- CVE-2021-30190
  - Base Score: 9.8 (Critical)
- CVE-2021-30191
  - Base Score: 7.5 (High)
- CVE-2021-30192
  - Base Score: 9.8 (Critical)
- CVE-2021-30193
  - Base Score: 9.8 (Critical)
- CVE-2021-30194
  - Base Score: 9.1 (Critical)
- CVE-2021-30195
  - Base Score: 7.5 (High)

Published: 20 Jul 2021
Last Updated: 20 Jul 2021

2 Summary

The compact systems CS351E and CS351S and the communication module KE350G with integrated PLC contain technology from CODESYS GmbH. The manufacturer CODESYS GmbH published security bulletins [1], [2] about a weakness in the protocol for the communication between the PLC runtime and clients. By exploiting these vulnerabilities, attackers can send crafted communication packets which may result in a denial of service condition or allow in worst case remote code execution.

3 Affected Products

- Compact system CS351E-D IL, firmware version V2.300 <= V2.800
- Compact system CS351E-G IL, firmware version V2.300 <= V2.800
- Compact system CS351S-D IL, firmware version V2.300 <= V2.800
- Compact system CS351S-G IL, firmware version V2.300 <= V2.800
- Communication module KE350G IL, firmware version V2.300 <= V2.800

4 Solution and Mitigations

Bosch Rexroth recommends to operate the product in a closed (machine) network with no access to the internet and implement the following compensatory measures:

- Minimize network exposure and ensure that the products are not accessible via the Internet.
- Network segmentation / Firewall: Isolate affected products from the corporate network.
- If remote access is required, use secure methods such as virtual private networks (VPNs).
- Activate and apply user management and password features.

With these measures the risk of exploitation of these vulnerabilities is very low.

5 Vulnerability Details

5.1 CVE-2021-30186

CVE description: CODESYS V2 runtime system SP before 2.4.7.55 has a Heap-based Buffer Overflow.

- Problem Type:
  - CWE-787
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

5.2 CVE-2021-30188

CVE description: CODESYS V2 runtime system SP before 2.4.7.55 has a Stack-based Buffer Overflow.

- Problem Type:
  - CWE-787
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.3 CVE-2021-30189

CVE description: CODESYS V2 Web-Server before 1.1.9.20 has a Stack-based Buffer Overflow.

- Problem Type:
  - CWE-787
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.4 CVE-2021-30190

CVE description: CODESYS V2 Web-Server before 1.1.9.20 has Improper Access Control.

- Problem Type:
  - CWE-668
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.5 CVE-2021-30191

CVE description: CODESYS V2 Web-Server before 1.1.9.20 has a a Buffer Copy without Checking the Size of the Input.

- Problem Type:
  - CWE-120
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

5.6 CVE-2021-30192

CVE description: CODESYS V2 Web-Server before 1.1.9.20 has an Improperly Implemented Security Check.

- Problem Type:
  - CWE-863
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.7 CVE-2021-30193

CVE description: CODESYS V2 Web-Server before 1.1.9.20 has an Out-of-bounds Write.

- Problem Type:
  - CWE-787
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.8 CVE-2021-30194

CVE description: CODESYS V2 Web-Server before 1.1.9.20 has an Out-of-bounds Read.

- Problem Type:
  - CWE-125
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
  - Base Score: 9.1 (Critical)

5.9 CVE-2021-30195

CVE description: CODESYS V2 runtime system before 2.4.7.55 has Improper Input Validation.

- Problem Type:
  - CWE-125
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

5.10 Remark

Vulnerability classification has been performed using the CVSS v3.1 scoring system. The CVSS environmental score is specific to each customer's environment and should be defined by the customer to attain a final scoring.

6 Additional Resources

[1] Codesys Security Advisory ID 2021-06:
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14725&token=08691519ef764b252630759eff925890176ecd78&download

[2] Codesys Security Advisory ID 2021-07:
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14726&token=553da5d11234bbe1ceed59969d419a71bb8c8747&download

7 Revision History

20 Jul 2021: Initial Publication