Security Advisory

Multiple vulnerabilities in libexpat affecting PRC7000

1 Advisory Information

Advisory ID: BOSCH-SA-200802

CVE Numbers and CVSS v3.1 Scores:

- CVE-2024-45490
  - Base Score: 9.8 (Critical)
- CVE-2024-45491
  - Base Score: 9.8 (Critical)
- CVE-2024-45492
  - Base Score: 9.8 (Critical)

Published: 02 Oct 2024

Last Updated: 02 Oct 2024

2 Summary

Multiple vulnerabilities were discovered in the open source library "libexpat", affecting the XML parser functionality. These vulnerabilities allow for integer overflows and invalid negative values for buffer sizes. As this may affect the "Import" and "Restore" functionality - which use libexpat to parse XML files - of the device, updating the firmware is strongly advised.

3 Affected Products

- PRC7000
  - CVE-2024-45490, CVE-2024-45491, CVE-2024-45492
    - Version(s): all 1.10.0.x - 1.10.5.x
    - Version(s): all 1.11.0.x - 1.11.11.x
    - Version(s): 1.11.12.0 <= 1.11.12.5
    - Version(s): 1.11.13.0 <= 1.11.13.3
    - Version(s): 1.11.14.0 <= 1.11.14.1

4 Solution

Update the PRC7000 firmware to one of the following versions.

- Version 1.11.12.6
- Version 1.11.13.4
- Version 1.11.14.2

Please note that versions older than 1.11.12.x will not be fixed, affected devices should be updated to 1.11.12.6 at least.

5 Mitigation

The issue can only be mitigated by employing strict restrictions on both physical access and (remote) network access to the device, preventing possibly malicious actors to access the device.

6 Vulnerability Details

6.1 CVE-2024-45490

CVE description: An issue was discovered in libexpat before 2.6.3. xmlparse.c does not reject a negative length for XML_ParseBuffer.

- Problem Type:
  - CWE-611: Improper Restriction of XML External Entity Reference
- 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)

6.2 CVE-2024-45491

CVE description: An issue was discovered in libexpat before 2.6.3. dtdCopy in xmlparse.c can have an integer overflow for nDefaultAtts on 32-bit platforms (where UINT_MAX equals SIZE_MAX).

- Problem Type:
  - CWE-190: Integer Overflow or Wraparound
- 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)

6.3 CVE-2024-45492

CVE description: An issue was discovered in libexpat before 2.6.3. nextScaffoldPart in xmlparse.c can have an integer overflow for m_groupSize on 32-bit platforms (where UINT_MAX equals SIZE_MAX).

- Problem Type:
  - CWE-190: Integer Overflow or Wraparound
- 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)

7 Remarks

7.1 Security Update Information

With respect to Directive (EU) 2019/770 and Directive (EU) 2019/771 and their national transposition laws, please note:

It is your responsibility to download and/or install any security updates provided by us, for example to maintain product or data security. If you fail to install a security update provided to you within a reasonable period of time, we will not be liable for any product defect solely due to the absence of such security update.

Alternatively, we are entitled to directly download and/or install security updates regardless of your settings. In these cases, we will provide you with the relevant information, e.g., in this security advisory.

7.2 CVSS Scoring

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.

8 Revision History

02 Oct 2024: Initial Publication