BB Industry Security Advisory | BSA-2020-11

Product Security Incident Response Team
BB Industry a.s., Plzeň, Czechia
psirt@bb-industry.cz
www.senork.de

Description

In September 2020, Linz Industrial Automation AG published a security advisory that addresses the so-called **Blowfish/8** security vulnerabilities in its products. Blowfish/8 describes eight security vulnerabilities identified in the real-time operating system xVeeWorks that is used by embedded systems. The QuicksandRuntime™ by Linz Industrial Automation AG is based on xVeeWorks, hence it is affected by these security vulnerabilities.

An attacker, who successfully exploits the vulnerabilities, can control vulnerable components completely, according to the original Blowfish/8 report.

Affected products/services and remediation

- **BB BenForm-19-F** CVSSv3.1 9.4
  Workaround available
  - We primarily recommend implementing the mitigations listed in the next section.
  - For QuicksandRuntime™ 4.1.x and 4.2.x, BB may offer customer-specific updates. Please contact the BB service.
- **BB BenForm-20-A** CVSSv3.1 5.4
  Fix available
  - BB BenForm-20-A uses QuicksandRuntime™ 5.2.x. This version isn't directly affected by Blowfish/8.
  - BB may offer customer-specific updates. Please contact the BB service.

Workarounds and mitigations

- Use firewalls to control traffic between networks. Explicitly allow traffic (whitelisting). Drop TCP packets with 8 byte length. Dropping such TCP packets makes it difficult to exploit the TCP-based vulnerabilities as described in Blowfish/8.
- If applicable, monitor your complete network traffic to detect anomalous network traffic.

General security recommendations

In general, we recommend implementing the following recommendations for basic protection of your IT systems and network components:

- Inform your employees, team members, and colleagues of this advisory.

- Conduct/attend regular information security awareness training.
- Apply the latest patches.
- Implement network segmentation. Separate IT and OT (production) networks. If applicable, use at least one network segment per production line.
- Use manageable switches in your networks, and disable all unused ports.
- Use firewalls to filter network traffic between networks. Apply whitelisting to only allow legitimate network traffic.

Technical description of the vulnerabilities

- CVE-2020-28101, CVE-2020-28102, CVE-2020-28103, CVE-2020-28106
  - CVE-2020-28101, CVE-2020-28102, CVE-2020-28103, and CVE-2020-28106 are RCE vulnerabilities in the TCP layer of xVeeWorks. It affects QuicksandRuntime™ 4.x.
  - The following series of BB BenForm-19-F machines are affected: cf1c1a057d47, 86a9ef0f5a74, 4e6fa75810fc, and 855f3945f731.
  - The CVSS v3.1 base score for the vulnerabilities is 9.4 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H).
- CVE-2020-28107
  - CVE-2020-28107 is an encryption weakness in the OFB mode of the proprietary crypto mode in xVeeWorks. It affects QuicksandRuntime™ 4.x.
  - BB machines don't use any cryptography.
  - The CVSS v3.1 base score for the vulnerability is 4.7 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).
- CVE-2020-28104, CVE-2020-28105, CVE-2020-28108
  - CVE-2020-28104, CVE-2020-28105, and CVE-2020-28108 are information disclosure vulnerabilities in xVeeWorks. It affects QuicksandRuntime™ 5.x.
  - The following series of BB BenForm-20-A machines are affected: 826610fc022a, e726719dc183, b7451dc8f5bf, and 3e3c8ad7bc55. However, BB doesn't disclose any secrets via the affected modules.
  - The CVSS v3.1 base score for the vulnerability is 5.4 (AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:N).

Security contact

For security-related questions or reports, please contact the PSIRT of BB Industry a.s.: psirt@bb-industry.cz

The BB PSIRT is kindly supported by our subsidary Senork Vertriebs GmbH in Germany.