SIDEL SECURITY ADVISORY

Wibu-Systems - CodeMeter

SSA-2020-02

V1.0

Several vulnerabilities have been disclosed by **Wibu-Systems** in September 2020. These vulnerabilities impact CodeMeter Runtime, a license manager.

Among industrial control system (ICS) vendors, Wibu-Systems' CodeMeter is integrated into products from vendors who have a significant customer presence in industries such as pharmaceuticals, manufacturing, automotive developers, and many others. It provides a full-scale license management solution and antipiracy protection, in addition to other encryption guarding the intellectual property of companies worldwide.

Six vulnerabilities have been published, of which two are considered critical with a Common Vulnerability Scoring System (CVSS v3) score greater than or equal to 9 and four are considered important with 9 > CVSS v3 score > 7.

The following versions of CodeMeter Runtime are affected:

- All versions prior to 7.10a are affected by CVE-2020-14509 and CVE-2020-14519
- All versions prior to 7.10a are affected by CVE-2020-14517
- All versions prior to 7.10 are affected by CVE-2020-16233
- All versions prior to 6.81 are affected by CVE-2020-14513
- All versions prior to 6.90 are affected by CVE-2020-14515 when using CmActLicense update files with CmActLicense Firm Code

For Sidel equipment and services, the probability of being exploited is medium. Specific actions are required to ensure your best protection.

1 IMPACT ON SIDEL EQUIPMENT AND RECOMMENDED ACTIONS

1.1 Risks on Sidel Equipment and Services

Successful exploitation of these vulnerabilities could allow an attacker to alter and forge a license file, cause a denial-of-service condition, potentially attain remote code execution, read heap data and prevent normal operation of third-party software dependent on the CodeMeter.

To keep ensuring the security of our products, Sidel has taken the necessary measures to assess linked equipment and services. In the meantime, customers who have the potential to be affected should implement cybersecurity best practices throughout their operations for the best protection from the exploitation of these vulnerabilities.

As of today, two of our vendors, Copa-Data and Rockwell, have been impacted by these vulnerabilities.

1.2 Criticality and recommendations

- Critical vulnerabilities have a CVSS v3 of at least 9 (10.0 is the maximum rating).
- Proofs of concept that would show the existence of an exploitation of one of these vulnerabilities are not available.
- The official fix is available from Wibu-Systems.

Recommended measures, according to the affected equipment and level of risk, are as follows:

Affected equipment and services	Risk of exploitation*	Recommended actions
Blower and Filler machines with HMI template up to version V4.03.02	**Medium**	• Install the CodeMeter Runtime 7.10a version • Ensure in-depth defence by applying the generic compensating mitigations listed below • Contact Sidel for further assistance
Sidel machines with Rockwell PanelPC running FactoryTalk Activation Manager v4.05.00 and earlier	**Medium**	• Update FactoryTalk Activation Manager to version V4.05.01 • Ensure in-depth defence by applying the generic compensating mitigations listed below • Contact Sidel for further assistance
Sidel Pasteurisers and Bottlewashers machines with HMI running Copa Data Zenon up to version 7.6	**Medium**	• Install the CodeMeter Runtime 7.10a version • Ensure in-depth defence by applying the generic compensating mitigations listed below • Contact Sidel for further assistance
Sidel Palletiser machines with HMI running Copa Data Zenon up to version 7.6	**Medium**	• Apply the specific compensating mitigation below • Ensure in-depth defence by applying the generic compensating mitigations listed below • Contact Sidel for further assistance
Other end of Line Sidel machines with HMI running Copa Data Zenon up to version 7.6	**Medium**	• Apply the specific compensating mitigation below • Ensure in-depth defence by applying the generic compensating mitigations listed below • Contact Sidel for further assistance

* Assessment of risk is based on use case analysis.

1.3 Specific compensating mitigations

- Block traffic to port TCP/22350 to control networks and monitor any traffic on this specific port.
- Apply host firewall rules as well to block inbound communication on port TCP/22350.

1.4 Generic compensating mitigations

To optimise the security level, Sidel highly recommends that customers take the following actions:

- Consider locating control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Consider locating devices behind firewalls capable of deep packet inspection with rulesets limiting access to approved protocols and functions and to only those devices and endpoints requiring access.
- Install physical controls so no unauthorised personnel can access your industrial control and safety systems, components, peripheral equipment and networks.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in terminals or any node connected to these networks.
- Never allow laptops that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimise network exposure for all control system devices and systems and ensure that they are not accessible from the Internet (a tool like Shodan can be used to assess this exposure).

- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognise that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

2 TECHNICAL DETAILS OF THE VULNERABILITIES

- CVE-2020-14509 has been assigned to this vulnerability. A CVSS v3 base score of 10.0 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). Multiple memory corruption vulnerabilities exist where the packet parser mechanism does not verify length fields. An attacker could send specially crafted packets to exploit these vulnerabilities.
- CVE-2020-14517 has been assigned to this vulnerability. A CVSS v3 base score of 9.4 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H). Protocol encryption can be easily broken and the server accepts external connections, which may allow an attacker to remotely communicate with the CodeMeter API.
- CVE-2020-14519 has been assigned to this vulnerability. A CVSS v3 base score of 8.1 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H). This vulnerability allows an attacker to use the internal WebSockets API via a specifically crafted Java Script payload, which may allow alteration or creation of license files when combined with CVE-2020-14515.
- CVE-2020-14513 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). CodeMeter and the software using it may crash while processing a specifically crafted license file due to unverified length fields.
- CVE-2020-14515 has been assigned to this vulnerability. A CVSS v3 base score of 7.4 has been calculated; the CVSS vector string is (AV:L/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:H). There is an issue in the license-file signature checking mechanism, which allows attackers to build arbitrary license files, including forging a valid license file as if it were a valid license file of an existing vendor. Only CmActLicense update files with CmActLicense Firm Code are affected. CVE-2020-16233 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). An attacker could send a specially crafted packet that could have the server send back packets.

3 FURTHER REFERENCES

- https://us-cert.cisa.gov/ics/advisories/icsa-20-203-01
- https://www.wibu.com/support/security-advisories.html
- https://www.copadata.com/fileadmin/user_upload/faq/files/CD_SVA_2020_1.pdf
- https://www.claroty.com/2020/09/08/blog-research-vendors-affected-by-wibu-codemeter-vulnerabilities/

4 CHANGELOG

- **V1.0**: November 18th, 2020 - Initial publication