SIDEL SECURITY ADVISORY

Siemens SIMATIC S7

SSA-2021-02

V1.0

A vulnerability was disclosed by **Siemens** in May 2021. This vulnerability, is considered as high with a Common Vulnerability Scoring System (CVSS v3.1) score of 8.1 impact on the SIMATIC S7-1200 and S7-1500 CPU Families

SIMATIC S7-1200 and S7-1500 CPU products contain a memory protection bypass vulnerability that could allow an attacker to write arbitrary data and codes in protected memory areas or read sensitive data to launch further attacks.

The following products and versions are affected:

- SIMATIC Drive Controller family: All versions < V2.9.2
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions
- SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants): All versions
- SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.5.0
- SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.9.2
- SIMATIC S7-1500 Software Controller: All versions
- SIMATIC S7-PLCSIM Advanced: All versions < V4.0

For Sidel equipment, the probability of being exploited is considered low as no exploitation code exists or is actively used by threat actors. Specific actions are recommended to ensure your best protection.

1 IMPACT ON SIDEL EQUIPMENT AND RECOMMENDED ACTIONS

1.1 Risks to Sidel Equipment and Services

Affected devices are vulnerable to a memory protection bypass through a specific operation. A remote, unauthenticated attacker with network access to Port 102/TCP could write arbitrary data and codes in protected memory areas or read sensitive data to launch further attacks.

To continue ensuring the security of our products, Sidel has taken the necessary measures to assess all linked equipment and services. In the meantime, customers should ensure that they implement cybersecurity best practices throughout their operations to protect against the exploitation of these vulnerabilities.

1.2 Criticalities and recommendations

- Score CVSS v3.1: 8.1

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

Equipment and Services Affected	Risk of exploitation*	Recommended Actions
Sidel Pasteuriser Swing, Bottlewasher Hydra ad Pasteuriser C	Low	▪ Contact Sidel for further assistance to update to V2.9.2 ▪ Ensure in-depth defence by applying the generic compensating mitigations linked below
Other Sidel equipment using the S7-1200 and S7-1500 CPU families	Low	▪ Contact Sidel for further assistance ▪ Ensure in-depth defence by applying the generic compensating mitigations linked below

* Assessment of risk is based on use case analysis.

1.3 Generic compensating mitigations

To optimise security levels, Sidel highly recommends customers take the actions detailed in our guidelines to ensure an in-depth defence:

2 TECHNICAL DETAILS OF THE VULNERABILITIES

- CVE-2020-15782 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:H/PR:N/UI:N/S:U/C:H/I:H/A:H). The devices affected are vulnerable to a memory protection bypass through a specific operation. A remote, unauthenticated attacker with network access to Port 102/TCP could write arbitrary data and codes in protected memory areas or read sensitive data to launch further attacks.

3 FURTHER REFERENCES

- https://cert-portal.siemens.com/productcert/pdf/ssa-434534.pdf
- https://us-cert.cisa.gov/ics/advisories/icsa-21-152-01

4 CHANGELOG

- **V1.0**: June 10th, 2021 - Initial publication