SIDEL SECURITY ADVISORY

PTC Kepware KEPServerEX

SSA-2021-01

V1.0

Several vulnerabilities have been disclosed by **PTC** in December 2020. These vulnerabilities impact the software Kepware KEPServerEX.

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

The following versions of Kepware KEPServerEX are affected:

- Version 6.6
- Version 6.7
- Version 6.8
- Version 6.9

For Sidel equipment and services, the probability of being exploited is low. Specific actions are recommended 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 lead to a server crashing, a denial-of-service condition, data leakage, or remote code execution.

To continue ensuring the security of our products, Sidel has taken the necessary measures to assess 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 Criticality and recommendations

- Score CVSS v3: 9.8

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

Affected Equipment and Services	Risk of exploitation*	Recommended Actions
EIT Servers running Kepware KEPServerEX versions 6.6, 6.7, 6.8 or 6.9, and with OPC UA server role enabled and accessible over the network	Low	▪ Contact Sidel for further assistance ▪ Ensure in-depth defence by applying the generic compensating mitigations linked below ▪ For version 6.6 upgrade to version 6.6.362.0 ▪ For version 6.7 upgrade version 6.7.1067.0 ▪ For version 6.8 upgrade version 6.8.838.0 ▪ For version 6.9 upgrade to version 6.9.584.0

* Assessment of risk is based on use case analysis.

1.3 Generic compensating mitigations

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

2 TECHNICAL DETAILS OF THE VULNERABILITIES

- CVE-2020-27265 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated. The CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). The affected products are vulnerable to a stack-based buffer overflow. Opening a specifically crafted OPC UA message could allow an attacker to crash the server and remotely execute code.

- CVE-2020-27263 has been assigned to this vulnerability. A CVSS v3 base score of 9.1 has been calculated. The CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H). The affected products are vulnerable to a heap-based buffer overflow. Opening a specifically crafted OPC UA message could allow an attacker to crash the server and potentially leak data.

- CVE-2020-27267 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). The affected products are vulnerable to a use-after-free vulnerability, which may allow an attacker to create and close OPC UA connections at a high rate that may cause a server to crash.

3 FURTHER REFERENCES

- https://us-cert.cisa.gov/ics/advisories/icsa-20-352-02

4 CHANGELOG

- **V1.0**: January 26th, 2021 - Initial publication