SIDEL SECURITY ADVISORY

RIPPLE20

SSA-2020-01

V2.0

Ripple20 is a new set of vulnerabilities that was disclosed by the security company JSOF in June 2020. These vulnerabilities are linked to the implementation of Treck's TCP/IP stack, which is used in many embedded systems and connected objects, including industrial equipment.

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

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

1 IMPACT ON SIDEL EQUIPMENT AND RECOMMENDED ACTION

1.1 Risks on Sidel Equipment and Services

In case of a cyberattack, Ripple20 can cause:

- Remote execution of arbitrary code
- Remote denial of service
- Breach of data integrity
- Breach of data confidentiality

To keep on ensuring the security of our products, Sidel has taken the necessary measures to assess linked equipment and services. In the meantime, customers should implement cyber-security best practices throughout their operations for the best protection from the against the exploitation of these vulnerabilities.

As of today, 2 of our vendors, Schneider Electric and Rockwell Automation are confirmed to have been impacted by Ripple20.

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 publicly available.

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

Affected Equipment and Services	Risk of exploitation*	Recommended Action
Sidel machines that contain Schneider Electric components (Power Logic PM5320, PM5560)	**Low** if components are on isolated machine network **Medium** if components are connected to customer network	• Keep the machine network isolated • Apply the compensating mitigations listed below • Contact Sidel for further assistance
Sidel machines that contain Nematron HMI from Delta Compact (DC) and Formula Series (IF) (DC94F8-PFExxx41, DC94F8-KFExxx41, DC94F8-HFExxx41, DC94F8-GDBxxx41, IF5106-S5xxxxx34, IF5106-H5xxxx34, IF5106-F4xxxxx4, IF5306-H5xxxx34)	**Low** for isolated HMI **Medium** for HMI connected on customer network	• Apply the compensating mitigations listed below • Contact Sidel for further assistance
Sidel machines that contain Rockwell components (1794-AENTR Series A, 1732E-16CFGM12QCR, Kinetix 5500, Kinetix 5700, 1732E-16CFGM12R/B, 1794-AENTR Series A, 1732E-IB16M12R2	**Low** if components are on isolated machine network **Medium** if connected to customer network	• Apply the compensating mitigations listed below • Contact Sidel for further assistance
Sidel line supervisor EIT v5 and later running on HP Servers ProLiant Gen7 and Dell PowerEdge Series	**Low** if HP iLO or Dell iDRAC modules are not connected	• As per our standard installation procedures iLO is not connected. If customer has decided to use them, we recommend to return to original setup and manage the server through OS managed NIC • Apply the compensating mitigations listed below • Contact Sidel for further assistance

* Assessment of risk is based on use case analysis.

1.3 Compensating mitigations

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

- Consider locating the 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 only, and only to those devices and endpoints requiring access.
- Consider blocking network attacks via deep packet inspection. In some cases, modern switches, routers and firewalls will drop malformed packets with no additional configuration. It is recommended that such security features are not disabled. Below is a list of possible mitigations that can be applied as appropriate to your network environment.

- Normalise or reject IP fragmented packets (IP Fragments) if not supported in your environment.
- Disable or block IP tunnelling, both IPv6-in-IPv4 or IP-in-IP tunnelling if not required.
- Block IP source routing and any IPv6 deprecated features like routing.
- Enforce TCP inspection and reject malformed TCP packets.
- Block unused ICMP control messages such as MTU and Address Mask updates.
- Normalise DNS through a secure recursive server or application layer firewall.
- Ensure that you are using reliable OSI layer 2 equipment (Ethernet).
- Provide DHCP/DHCPv6 security with features like DHCP snooping.
- Disable or block IPv6 multicast if not used in switching infrastructure.

- Install physical controls so no unauthorized 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 CRITICAL AND IMPORTANT VULNERABILITIES

- **CVE-2020-11896** [Score CVSS v3: 10.0]: Fragmented UDP datagrams over multiple IP packets can allow remote arbitrary code execution or remote denial of service on equipment with IP Tunnelling enabled.

- **CVE-2020-11897** [Score CVSS v3: 10.0]: A vulnerability allowing remote execution of arbitrary code has been discovered in Treck's TCP/IP stack. An attacker can exploit this vulnerability by sending specially designed IPv6 packets.

- **CVE-2020-11898** [Score CVSS v3: 9.1]: A vulnerability due to incorrect handling of the length of a parameter has been discovered in the IPv4 / ICMPv4 component. An attacker can exploit this vulnerability in order to access sensitive information.

- **CVE-2020-11901** [Score CVSS v3: 9.0]: A vulnerability allowing remote execution of arbitrary dcode has been discovered in Treck's TCP/IP stack. An attacker can exploit this vulnerability by sending a specially designed DNS response. According to the researchers who discovered the Ripple20 vulnerabilities, this is the most important vulnerability despite its CVSS score of 9.0 and it can allow an attacker to take control of a device from an external network without being detected by security devices.
- **CVE-2020-11900** [Score CVSS v3: 8.2]: A "use-after-free" vulnerability has been discovered in the IPv4 tunnelling component. It can allow an attacker to cause a denial of service or arbitrary code execution.

- **CVE-2020-11902** [Score CVSS v3: 7.3]: An out-of-bounds read vulnerability has been discovered in the IPv6OverIPv4 tunnelling component. It is due to a validation fault when processing a packet sent by an unauthorized network.

3 FURTHER REFERENCES

- https://www.jsof-tech.com/ripple20/
- https://kb.cert.org/vuls/id/257161
- https://www.se.com/ww/en/download/document/SESB-2020-168-01
- https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp
- https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1126896

4 CHANGELOG

- **V1.0**: July 12th, 2020 - Initial publication
- **V2.0**: September 23rd, 2020 - Added list of impacted Sidel machines