CYBER SECURITY NOTIFICATION

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by Synergy Systems & Solutions (SSS).

SSS provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall SSS or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if SSS or its suppliers have been advised of the possibility of such damages.

Vulnerability Summary

VAPT Team, C3i Center, IITK, UP, India, vide their notification dated 13-Jan-2020, reported following vulnerabilities in HUSKY RTU 6049-E70.

1. An information exposure is the intentional or unintentional disclosure of information to an actor that is not explicitly authorized to have access to that information. An attacker can read sensitive information over the SNMP protocol.
2. Incorrect Permissions, which could cause a network configuration changes in the device through the SNMP communication.

Affected Products

SSS have investigated the reported vulnerabilities and identified the following products affected under this notification –

- HUSKY RTU 6049-E70, with firmware versions 5.0 and above.

The issue has been identified to be in the SNMP agent service provided by the RTU. The information provided under SNMP can be unintentionally disclosed to an unauthorized actor. However, no configuration changes can be affected through this facility, as RTU provides a read-only service.

Mitigating Factors

Following recommendations shall be implemented to avoid exposure to risks outlined in this outlined in this notification –

1. Customers are encouraged to implement network segmentation and firewall policies in their network to reduce exposure of the RTU to uncontrolled and unprotected access. Implement policies to block all unauthorized access to SNMP port 161/UDP.
2. Recommended security practices and firewall configurations can help protect an industrial control network from attacks that originate from outside the network. Such practices include that protection, control & automation systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Protection, control & automation systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Block all non-trusted IP communications.
3. For applications, not requiring SNMP monitoring, it is recommended to disable the feature through the RTU configuration.
4. If possible, setup SSL tunnel between RTU and control center to restrict access to the RTU.

The impact of the vulnerabilities above can be greatly reduced by implementing a firewall to restrict external network connectivity to the affected devices.

Acknowledgements

SSS recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2020-7801 CVE-2020-7802	VAPT Team (C3i IITK, UP, India)

Support

For additional information and support please contact support@s3india.com for further information.