Vulnerability of Information Disclosure, Information Tampering, Unauthorized Operation and Denial-of-Service (DoS) between MELSEC iQ-R, iQ-F, Q, L and FX series CPU modules and GX Works3/GX Works2

June 23, 2020
Mitsubishi Electric Corporation

■Overview

There is a vulnerability of information disclosure, information tampering, unauthorized operation and denial-of-service (DoS) due to cleartext communication between MELSEC iQ-R, iQ-F, Q, L and FX series CPU modules and GX Works3/GX Works2 (CWE-319). When performing communication via untrusted networks or hosts, there are risks of communication data eavesdropping/tampering, unauthorized operation and denial-of-service (DoS) attacks from malicious attackers.

■Affected products

All versions of MELSEC iQ-R, iQ-F, Q, L and FX series CPU modules are affected.

■Description

There is a vulnerability due to cleartext communication between MELSEC iQ-R, iQ-F, Q, L and FX series CPU modules and GX Works3/GX Works2. The vulnerability (CVE-2020-5594) causes information disclosure, information tampering, unauthorized operation and denial-of-service (DoS) condition (CWE-319).

■Impact

There is a possibility of information disclosure, information tampering, unauthorized operation and denial-of-service (DoS) attacks from malicious attackers.

■Mitigation

When performing communication via untrusted networks or hosts, please encrypt the communication path by setting up a VPN to mitigate the impact of this vulnerability.

■Acknowledgements

Mitsubishi Electric would like to thank Shunkai Zhu, Rongkuan Ma and Peng Cheng from NESC Lab of Zhejiang University who reported this vulnerability.

■Contact information

Please contact your local Mitsubishi Electric representative.