Multiple Vulnerabilities in TCP/IP stack on MELSEC iQ-R Series Information/Network Module

Release date: Oct 29, 2020
Mitsubishi Electric Corporation

■Overview

Multiple vulnerabilities were found in the TCP/IP stack of MELSEC iQ-R Series EtherNet/IP Network Interface Module, PROFINET IO Controller Module, High Speed Data Logger Module, MES Interface Module and OPC UA Server Module. If these vulnerabilities are exploited by malicious attackers, the network functions of the products may enter a denial-of-service condition or malware may be executed. (CVE-2020-5653、CVE-2020-5654、CVE-2020-5655、CVE-2020-5656、CVE-2020-5657、CVE-2020-5658)

The versions of the MELSEC iQ-R Series EtherNet/IP Network Interface Module, PROFINET IO Controller Module, High Speed Data Logger Module, MES Interface Module and OPC UA Server Module affected by these vulnerabilities are shown below. Please take the countermeasures or mitigation measures for the corresponding products.

■CVSS

CVE-2020-5653	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score: 9.8
CVE-2020-5654	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score: 7.5
CVE-2020-5655	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score: 7.5
CVE-2020-5656	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score: 9.8
CVE-2020-5657	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	Base Score: 7.1
CVE-2020-5658	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	Base Score: 5.3

■Affected products

Affected products are as follows.

[MELSEC iQ-R Series EtherNet/IP Network Interface Module]
- RJ71EIP91: First 2 digits of serial number are "02" or before.

[MELSEC iQ-R Series PROFINET IO Controller Module]
- RJ71PN92: First 2 digits of serial number are "01" or before.

[MELSEC iQ-R Series High Speed Data Logger Module]
- RD81DL96: First 2 digits of serial number are "08" or before.

[MELSEC iQ-R Series MES Interface Module]
- RD81MES96N: First 2 digits of serial number are "04" or before.

[MELSEC iQ-R Series OPC UA Server Module]
- RD81OPC96: First 2 digits of serial number are "04" or before.

The serial number of module can be checked in "System Monitor" of GX Works3 (Fig. 1).

1. Launch GX Works3.
2. Select "Diagnostics"→"System Monitor" from "Menu bar".
3. Click "Product Information List" button in "System Monitor".

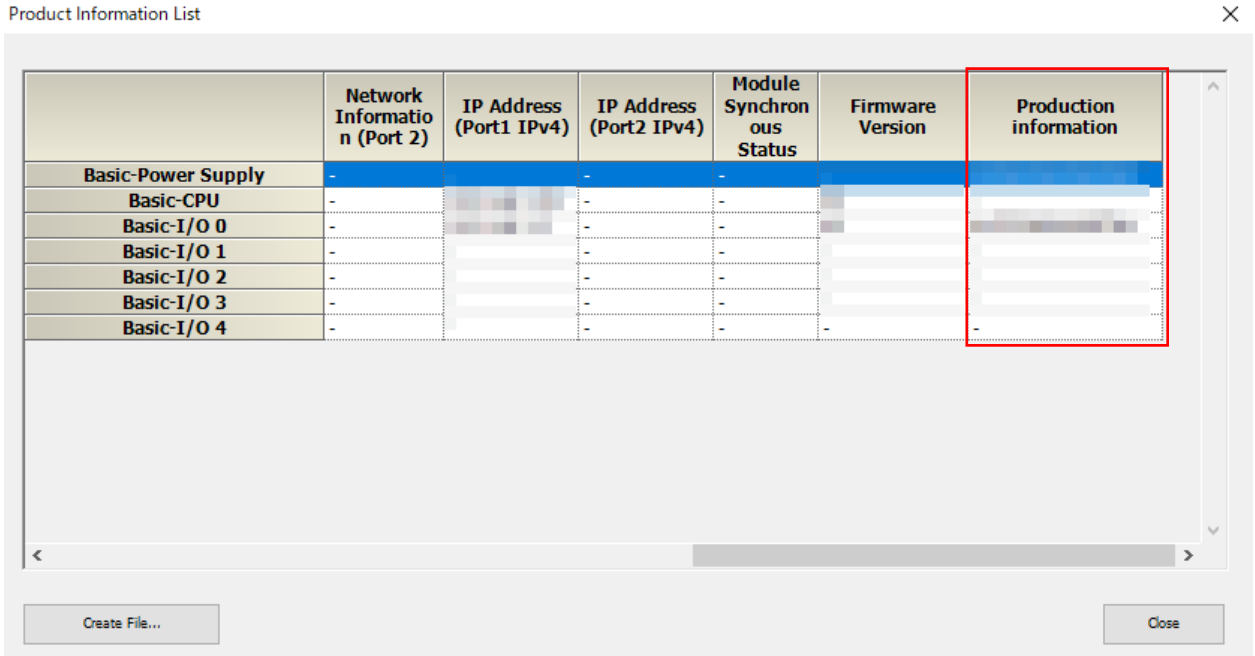

Fig.1 serial number check screen

■Description

The MELSEC iQ-R Series EtherNet/IP Network Interface module, PROFINET IO Controller Module, High Speed Data Logger Module, MES Interface Module and OPC UA Server Module have an Ethernet communication port to communicate with external devices. There are following multiple vulnerabilities in TCP/IP stack of the firmware in these modules. By receiving specially crafted packets from remote attackers, the network functions of the products may enter a denial-of-service condition or malware may be executed.

·Improper Restriction of Operations within the Bounds of a Memory Buffer (CWE-119) CVE-2020-5653
·Session Fixation (CWE-384) CVE-2020-5654
·NULL Pointer Dereference (CWE-476) CVE-2020-5655
·Improper Access Control (CWE-284) CVE-2020-5656
·Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') (CWE-88) CVE-2020-5657
·Resource Management Errors (CWE-399) CVE-2020-5658

■Impact

By receiving specially crafted packets from attackers, the network functions of the products may enter a denial-of-service condition or malware may be executed.

■Countermeasures

We have fixed the vulnerabilities at the following versions.

[MELSEC iQ-R Series EtherNet/IP Network Interface Module]
- RJ71EIP91: First 2 digits of serial number are "03" or later.

[MELSEC iQ-R Series PROFINET IO Controller Module]
- RJ71PN92: First 2 digits of serial number are "02" or later.

[MELSEC iQ-R Series High Speed Data Logger Module]
- RD81DL96: First 2 digits of serial number are "09" or later.

[MELSEC iQ-R Series MES Interface Module]
- RD81MES96N: First 2 digits of serial number are "05" or later.

[MELSEC iQ-R Series OPC UA Server Module]
- RD81OPC96: First 2 digits of serial number are "05" or later.

■Mitigations

Please restrict access to the product only from trusted networks and hosts.

■Contact information

Please contact your local Mitsubishi Electric representative.