Denial-of-Service Vulnerability in MELSEC iQ-R Series CPU Module

Release date: August 5, 2021
Mitsubishi Electric Corporation

■Overview

Denial-of-Service (DoS) vulnerability exists in MELSEC iQ-R series CPU modules due to Overly Restrictive Account Lockout Mechanism (CWE-645). A remote attacker could lockout a legitimate user by continusly trying login with incorrect password. (CVE-2021-20598)

The product models and firmware versions affected by this vulnerability are listed below.

■CVSS

CVE-2021-20598 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L Base Score:3.7

■Affected products

The following modules are affected:

Model name	Firmware Version
R08/16/32/120SFCPU	all versions
R08/16/32/120PSFCPU	all versions

■Description

Denial-of-Service (DoS) vulnerability due to Overly Restrictive Account Lockout Mechanism (CWE-645) exists in MELSEC iQ-R series CPU modules.

■Impact

MELSEC iQ-R series lockouts the user account when an incorrect password is entered in succession. A remote attacker could lockout a legitimate user by continusly trying login with incorrect password. Therefore, a legitimate user could not login.

■Mitigations/Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:

- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Use the IP filter function※1 to restrict the accessible IP addresses.

※1:MELSEC iQ-R Ethernet User's Manual(Application) Security "IP filter"

■Acknowledgement

Mitsubishi Electric would like to thank Ivan Speziale of Nozomi Networks Labs who reported this vulnerability.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

https://www.mitsubishielectric.com/fa/support/index.html