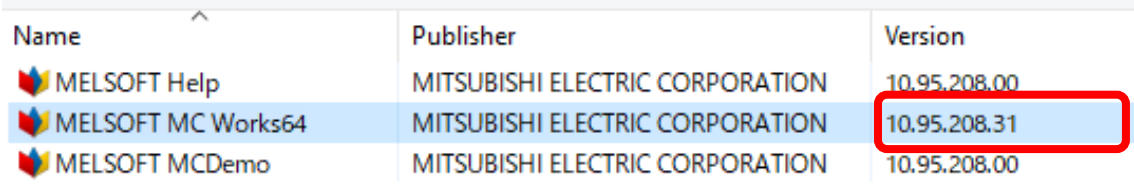
Denial of Service vulnerability and Remote Code Execution vulnerability in MC Works 64 and MC Works 32

June 18, 2020
Last Updated September 9, 2020
Mitsubishi Electric Corporation

■Overview
Multiple vulnerabilities have been found in MC Works64 and MC Works32. An attacker can cause a Denial of Service (DoS) or execute arbitrary code by sending specially crafted data. The following versions of MC Works64 and MC Works32 are affected by this issue. Please apply the security patch.

■Affected products
<products and version>
MC Works64: Version 4.02C (Version 10.95.208.31) (*1) and earlier
MC Works32: Version 3.00A (Version 9.50.255.02) (*1)
*1 Versions of MC Works64 and MC Works32 displayed in [Control Panel]-[Programs and Features].
Select Windows® Start menu, and then [Windows System Tools] → [Control Panel] → [Programs and Features]. After this operation, MC Works64 is displayed as "MELSOFT MC Works64" and MC Works32 is displayed as "Mitsubishi Electric MC Works".



Name	Publisher	Version
MELSOFT Help	MITSUBISHI ELECTRIC CORPORATION	10.95.208.00
MELSOFT MC Works64	MITSUBISHI ELECTRIC CORPORATION	10.95.208.31
MELSOFT MCDemo	MITSUBISHI ELECTRIC CORPORATION	10.95.208.00

<Version information>

■Description
The following 5 vulnerabilities have been found in MC Works64 and MC Works32.
(1) When MC Broker 64 in MC Works 64 or MC Broker32 in MC Works32 receives a specially crafted packet, it may enter a Denial of Service condition or execute arbitrary code remotely due to out-of-bounds write. (CWE-787)
(2) When MC Works64 platform service receives a specially crafted packet, it may enter a Denial of Service condition due to improper deserialization. (CWE-502)
(3) When MC Works64 Workbench Pack & Go function receives a specially crafted package, it may execute arbitrary code remotely due to improper deserialization. (CWE-502)
(4) When GridWorX server in MC Works64 receives a specially crafted message from a custom client function, it may disclose internal data, allow internal data tampering or execute arbitrary SQL command remotely. (CWE-94)
(5) When FrameWorX server in MC Works64 receives a specially crafted packet, it may enter a Denial of Service condition or execute arbitrary code remotely due to improper deserialization. (CWE-502)

■Impact
Successful exploitation of these vulnerabilities may allow remote code execution, denial of services, information disclosure or information tampering.

■Countermeasures
The security patch can be downloaded from "MC Works64 and MC Works32 SECURITY UPDATES" web page to update the software. This web page is hosted by ICONICS, a group company of Mitsubishi Electric.
<Security Patches for MC Works64 Version 4.00A - 4.02C>
MC Works64 Version 4.00A (Version 10.95.201.15)
MC Works64 Version 4.02C (Version 10.95.208.31)
MC Works64 Edge-computing Edition Version 4.00A_4.01B (Version 10.95.201.37)
MC Works64 Edge-computing Edition Version 4.02C (Version 10.95.208.31)
<MC Works64 Version 3.04E (Version 10.94.178.04) or earlier>
Please contact your local Mitsubishi Electric representative.
<Security Patch for MC Works32 Version 3.00A>
MC Works32 Version 3.00A (Version 9.50.255.02)

■Mitigations
If the above coutermeasures (software update) cannot be implemented, take the following defensive measures.
(1) Restrict network exposure for all control system devices or systems, and ensure that they are not accessible from untrusted networks and hosts.

(2) Locate control system networks and remote devices behind firewalls and isolate them from the business network.
(3) When remote access is required, use Virtual Private Network (VPN). VPN is effective for securing the connected devices.

■Contact information
Please contact your local Mitsubishi Electric representative.

■Update history
September 9, 2020
Added Security Patches for MC Works64 Version 4.00A – 4.02C.