Multiple vulnerabilities in MELSOFT iQ AppPortal

Release date: May 12. 2022
Mitsubishi Electric Corporation

■Overview

MELSOFT iQ AppPortal, provided by Mitsubishi Electric, is equipped with the server software VisualSVN Server. Multiple vulnerabilities have been found in the OSS (Open Source Software) used by VisualSVN Server. Exploits for these vulnerabilities may allow attacker to disclose or tamper with information with the product, cause a denial of service (DoS) conditions or execute malicious programs.

Versions of the MELSOFT iQ AppPortal affected by these vulnerabilities are listed below.

■CVSS

- CVE-2020-13938	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	Base Score:5.5
- CVE-2021-26691	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score:9.8
- CVE-2021-34798	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score:7.5
- CVE-2021-3711	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score:9.8
- CVE-2021-44790	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score:9.8
- CVE-2022-22720	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score:9.8
- CVE-2022-23943	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score:9.8
- CVE-2022-0778	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score:7.5

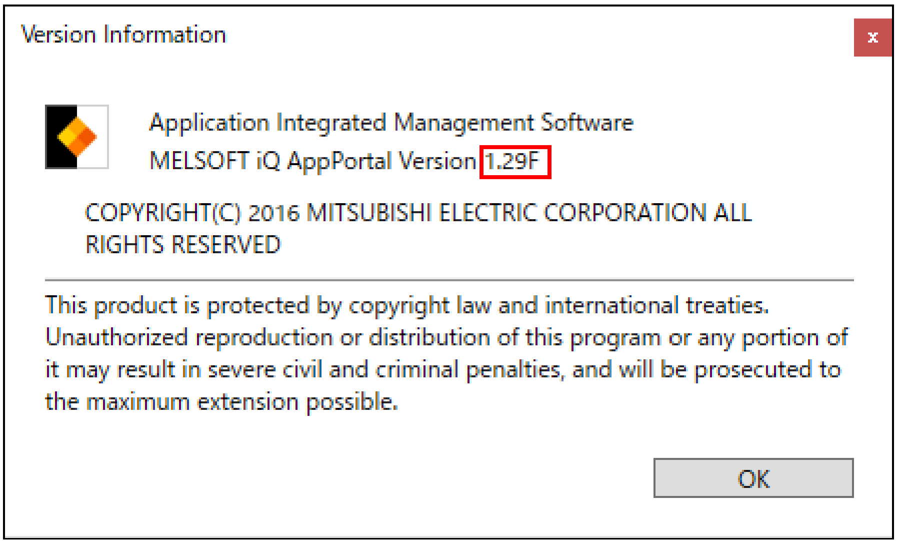
■Affected products

The affected product and versions are below.

products	Module Name	versions
MELSOFT iQ AppPortal	SW1DND-IQAPL-M	1.00A to 1.26C

How to check the version number you're using is below:

1. Start MELSOFT iQ AppPortal and select "Version Information" from the "Help" menu.
2. The following part of the window that appears is the version number of MELSOFT iQ AppPortal.(See Figure 1)



Application Integrated Management Software
MELSOFT iQ AppPortal Version 1.29F

COPYRIGHT(C) 2016 MITSUBISHI ELECTRIC CORPORATION ALL RIGHTS RESERVED

This product is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program or any portion of it may result in severe civil and criminal penalties, and will be prosecuted to the maximum extension possible.

Figure 1 : MELSOFT iQ AppPortal Version Information Window

■Description

The following vulnerabilities exist in the OSS (Open Source Software) used by VisualSVN Server, the server software equipped in MELSOFT iQ AppPortal:

The following vulnerabilities can result in a denial of service (DoS) condition:
- CVE-2020-13938: Missing Authorization (CWE-862)
- CVE-2021-34798: NULL Pointer Dereference (CWE-476)
- CVE-2022-0778: Loop with Unreachable Exit Condition ('Infinite Loop') (CWE-835)

The following vulnerabilities can result in information tampering, denial of service (DoS) conditions, or malicious programs execution:
- CVE-2021-26691: Out-of-bounds Write (CWE-787)

- CVE-2021-3711: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (CWE-120)
- CVE-2021-44790: Out-of-bounds Write (CWE-787)
- CVE-2022-23943: Out-of-bounds Write (CWE-787)

The following vulnerability can result in information disclosure, information tampering, or authentication bypass.

- CVE-2022-22720: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') (CWE-444)

■Impact

Exploits for these vulnerabilities may allow attacker to disclose or tamper with information with the product, cause a denial of service (DoS) conditions or execute malicious programs.

■Countermeasures

Download version 1.29F or later software from the following site and update the software.

https://www.mitsubishielectric.com/fa/#software

< How to Update>

1. Unzip the downloaded file (zip format).
2. Execute the file ″setup.exe″ located in the folder unzipped and install it.

■Workarounds

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

(1) Restrict network access from the computer installed the product so that it can be accessed only from trusted networks or hosts.
(2) Minimize user privilege for product users.
(3) Install an antivirus software in your personal computer installed the product.
(4) Please follow the Safety Precautions in the operating manual for the product.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >
https://www.mitsubishielectric.com/fa/support/index.html