HTTP Request Smuggling Vulnerability and IP Address Authentication Bypass Vulnerability in MELSOFT iQ AppPortal

Release date: February 21, 2023
Mitsubishi Electric Corporation

■Overview

MELSOFT iQ AppPortal, provided by Mitsubishi Electric, is equipped with the server software VisualSVN Server. If a user enables mod_proxy or mod_proxy_ajp in the VisualSVN Server settings, HTTP request smuggling vulnerability (CVE-2022-26377) and IP address authentication bypass vulnerability (CVE-2022-31813) exist in Apache HTTP Server used by VisualSVN Server. These vulnerabilities allow a malicious attacker to make unidentified impact, such as authentication bypass, information disclosure or denial of service (DoS), or bypass IP address authentication.

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

■CVSS[1]

CVE-2022-26377 :CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score: 7.5
CVE-2022-31813 :CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score: 9.8

■Affected products

The affected product and versions are below.

products	Module Name	versions
MELSOFT iQ AppPortal	SW1DND-IQAPL-M	1.00A to 1.29F

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)

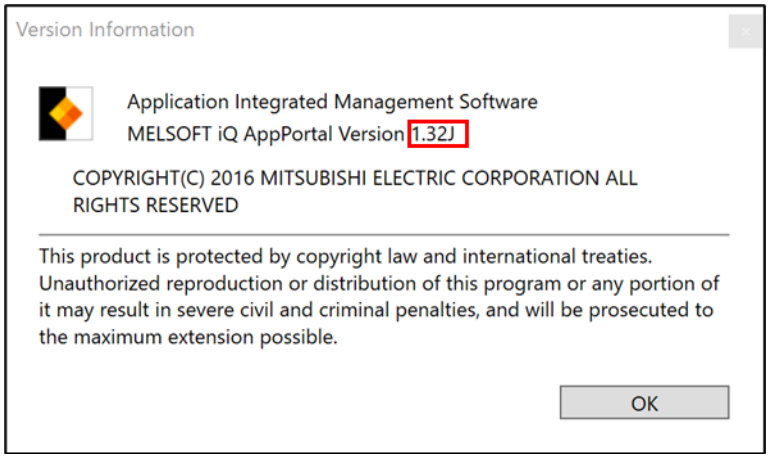

Figure 1:MELSOFT iQ AppPortal Version Information Window

■Description

HTTP request smuggling vulnerability (CVE-2022-26377) and IP address authentication bypass vulnerability (CVE-2022-31813) exist in the Apache HTTP Server used by VisualSVN Server, the server software included in the MELSOFT iQ AppPortal, if a user enables mod_proxy and mod_proxy_ajp in the VisualSVN Server settings:

The following flaw can result in unidentified impacts, such as authentication bypass, information disclosure or denial of service (DoS) condition:

CVE-2022-26377: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') (CWE-444)[2]

The following flaw can result in authentication bypass:

CVE-2022-31813: Insufficient Verification of Data Authenticity (CWE-345)[3]

■Impact

These vulnerabilities allow a malicious attacker to make unidentified impact, such as authentication bypass, information disclosure or denial of service (DoS), or bypass IP address authentication.

---

1 https://www.first.org/cvss/v3.1/specification-document
2 https://cwe.mitre.org/data/definitions/444.html
3 https://cwe.mitre.org/data/definitions/345.html

■Countermeasures

Download version 1.32J 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.

■Mitigations/Workarounds

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

<Workarounds>

(1) Disable mod_proxy and mod_proxy_ajp in the VisualSVN Server settings if possible.

<Mitigations>

(1) When a PC with the product installed need to access to the Internet, use a firewall or virtual private network(VPN), etc. to prevent unauthorized access.
(2) Use the PC using the product within a LAN and use a firewall, etc. to minimize connection to the network and restrict access only from trusted networks and hosts.
(3) Minimize user privilege for the product users.
(4) Install an antivirus software in the PC using the product.

■Contact information

Please contact your local Mitsubishi Electric representative.

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